Appendix of Notification of Bank Indonesia Number: 9/ 30 /DPNP dated 12 of December 2007

Appendix 1

GUIDELINES FOR THE IMPLEMENTATION OF RISK MANAGEMENT IN THE USE OF INFORMATION TECHNOLOGY BY COMMERCIAL BANKS

Directorate for Research and Banking Regulations

Table of Contents

PREFACE

To increase the efficiencies of banks' operational activities and the quality of banks's service to their customers, said Banks are expected to develop business strategies, amongst others by reaping the benefits of improvement of Information Technology (IT). Such strategy development will further promote new investments in Information Technology used in transaction and information processing. The ability of Banks in managing IT will determine the success in producing complete, accurate, updated, total, secure, consistent, punctual and relevant information. Therefore, the generated information is able to support the processes of decision making and the-operation of Bank's business.

On the other side of increasing the speed and accuracy of transactions as well as level of service to customers, the implementation of IT is also increasing risks such as operational, reputation, legal, compliance and strategic risks. This is the reason of expecting Banks to have an integrated risk management in identifying, measuring, monitoring and controlling risks. However, with regards to the variety of market conditions, structure, magnitude and complexity of the Bank's business, there are no single system of risk management that can be used for all Banks and thus every Bank has to develop their own proper risk management system in accordance to the functions and organization of the Bank's risk management.

These guidelines cover the risk management implementation principles that sholuld be-implemented by Banks to mitigate risks related to the management of IT. Banks with large and complex business scale should adopt more stringent measures in addition to the requirements in these guidelines. On the other hand, Banks with small and not so complex business scale may apply less stringent measures from those mentioned in these guidelines as long as the Bank has considered either the result of the risk assessment in the Bank's business activities, IT security profile or the result of cost and benefit analysis. Banks are also expected to implement the risk management framework in regards to the valid regulations, national and international standards as well as best practices, to ensure that adequate risk management has been implemented.

CHAPTER I
MANAGEMENT

1.1. INTRODUCTION

Bank's operational activities, including transactions processing and documentation are very dependent on the reliability of Information Technology (IT). Generated information is important in the decision making process by both internal and external parties. Therefore, IT must be managed effectively to maximize its effectiveness and to mitigate the-related risks of the implemented technologies.

Considering that IT is an important asset in operations which is enables a bank to increase the Bank's value and competitive edge and also bears some various inherent risks at the same time, encourages the further requirement for the Bank to implement IT Governance. The implementation of IT Governance is accomplished through an allignment of Information Technology Strategic Plan with Bank's business strategy, optimization of resources management, IT value delivery, performance measurement and effective risk management implementation. The success of the implementation of IT Governance depends much on the commitment of the board of commissioners and directors as well as the entire Bank's unit, of either IT Operations or users.

In relation to it, policies which contain the roles and responsibilities of the board of commissioners, directors and IT senior officials should exist in order to ensure the effective implementation of IT risk management.

1.2. INFORMATION TECHNOLOGY MANAGEMENT

1.2.1. Management Roles and Responsibilities

1.2.1.1. Board of Commissioners

In accordance with the Ordinance of Limited Holding, the functions of the Board of Commissioners are to observe policies of the directors in the Bank's operation as well as to provide advisory to the directors. Therefore the Board of Commissioners should have commitments, understand and take a part in any IT related activities. Responsibilities of the board of commissioners consist amongst others:

a. to direct, monitor and evaluate the IT Strategic Plan and Bank's policies related to the management of IT;
b. to conduct monitoring and to appraise compliance between policies and the implementation of risk management on IT usage;
c. to conduct evaluation on the planning and execution of an audit, to ensure that such audit is executed in sufficient frequency and scope, as well as conducting monitoring on the follow-ups of audit results;

d. to conduct evaluation on the management of reliable and effective IT Security in order to ensure the availability, confidentiality, accuracy/integrity of information.

1.2.1.2. Directors

Authorities and responsibilities for directors consist of:

a. determining IT Strategic Plan and short-term IT management/development in alligned with the Bank's strategic and annual plans;

b. determining adequate policies and procedures related to the management of IT and to communicate it effectively, to both IT organizers and business units. Furthermore the director overseeing Compliance Unit has to review those policies and procedures to ensure compliance to valid regulations;

c. reviewing, accepting and monitoring technology projects which significantly impacts on the Bank's operations and financial situations;

d. Ensuring:

   1) Existing IT applied by Bank are able to support the business development, Bank's business achievement and the continuation of service to customers;
   2) the availability of a unit whose function is to organize IT managed by the Bank (or used by the Bank if IT is managed by IT service provider);
   3) the previously determined policies and procedures as well as standards are implemented, reviewed and revised periodically;
   4) the availability of an Information Security Management System that is effective and properly communicated to all users and organizers of Information system;
   5) an implementation of risk management process in the use of IT is exist and conducted effectively and adequately in ways of:
      a) growing risk awareness from the management;
      b) having and communicating a clear understanding regarding the criteria and tolerable levels of risk (risk appetite) to IT users and organizers unit;
      c) having an understanding toward valid regulations;
      d) communicating significant risk transparently to IT users and organizers unit who deal with such risks; and
      e) developing organization structure along with descriptions of assignments and responsibilities that are able to manage the risks dealt comprehensively, systematically and integrally by the Bank.
   6) the availability of sufficient and competent human resources according to necessity;
   7) the existence of efforts to increase the competency of human resources related to the management of IT, amongst others through adequate education/training and education programs to increase awareness on information security;

8) the existence of a performance measuring system of IT management process, which can at least:
    a) support monitoring processes on implementation strategy;
    b) support completion of projects;
    c) optimize the application of investments on infrastructure and human resources;
    d) increase the performance of IT management process and the quality of service in conveying results of processes to users;
9) organization structure of IT related projects management are used to the maximum;

e. in the event of a Bank using a third party service, directors should ensure that the Bank has a written contract which governs the roles, relationships, obligations, and responsibilities from all contracting parties, as well as having assurance that the contract is a enforceable agreement and protects the interest of the Bank.

1.2.1.3. Information Technology Steering Committee

Banks must have an IT Steering Committee to assist the board of commissioners and directors in monitoring the IT related activities. The committee must consist at minimum:

a. A director who oversees Information Technology unit;
b. A director who oversees Risk Management unit;
c. An uppermost official who oversees IT Operations unit;
d. An uppermost official who oversees IT main users unit.

The mandatory to own an IT Steering Committee is also valid for Banks owned by foreign financial institutions. As for a branch office of foreign banks (KCBA), the functions of IT Steering Committee are able to be carried out by similar functions in the head office or regional office.

To perform its duty, the IT Steering Committee must possess an IT Steering Committee Charter which mentions the authorities and obligations of the committee.

To perform its duty effectively and efficiently, the committee should perform periodic meetings to discuss issues related to IT strategy, which are documented in the form of minutes of meetings.

The authority and obligation of IT Steering Committee is to provide, to the directors, recommendations which consist of at minimum:

a. Information Technology Strategic Plan in aligned with Bank's business strategy plan. In providing recommendations, the Committee should consider factors of efficiency,of effectiveness, as well as the following:

1) Road-map to achieve the requirements of IT that support the Bank's business strategy. Road map consist of the current state, future state, as well as steps to achieve said future state;
2) necessary resources;
3) benefits/ effects as the outcome of when the plan is implemented.

b. drafts of main IT policies and procedures, for example is the policy of IT security and IT related risk management;
c. accordance of agreed IT projects with IT Strategic Plan. The committee also determine priority status of critical IT projects (significant to Bank's operations), for example the changing of core Banking application, production server and network topology;
d. accordance of IT projects management with project charter which is agreed upon service level agreement. The committee should include the results of analysis from main IT projects in their recommendations, so as to enable directors' decisions making efficiently;
e. accordance of IT with the necessity of management information system which supports the Bank's business organization;
f. the effectiveness of steps taken to minimize risks on Bank's investments on IT, and so that said investments contribute to the achievements of the Bank's goal;
g. monitoring the IT performance, and the efforts of improving by detecting obsolete IT and measuring the effectiveness and efficiency of the implementation of IT security policies;
h. efforts to solve various problems related to IT, which can not be solved by users unit and organizers unit. The committee can facilitate the relationship of both unit;
i. sufficiency and allocation of the Bank's resources. If said resources are insufficient and the Bank will utilize services from another party to operate IT, the IT Steering Committee should ensure the Bank owns related policies and procedures.

1.2.1.4. Uppermost Official with the Obligation of Overseeing the IT

In its organization structure, Banks have to decide an uppermost official whose main responsibility is to oversee the IT. Such position may be hold by the director of IT or by chief of IT unit in accordance with the business complexity of the Bank. The main authority and responsibility of said IT official includes in minimum (but not limited to) the following:

a. drafting of IT policies, planning and budget;
b. implementing any and all IT policies and plans determined by the directors;
c. providing support of IT service allocation to user units to achieve its business targets responsively and promptly;

d. ensuring every information from the IT user units are well-protected from all sorts of disturbances which can cause losses from disclosures of important data/information;

e. ensuring sufficiency and effectiveness of IT policies and procedures as well as implementation of risk management, to identify, measure, assess and observe IT risks;

f. ensuring adequate monitoring have been incorporated in every development or modification of IT system;

g. providing IT management report periodically to the directors, and recommend actions to respond on IT weaknesses discovered if necessary ;

h. assessing the performance of the Bank's IT services, a such as percentage of the duration of downtime errors, security violations, project developments, implementation of Service Level Agreement (SLA) between IT unit and users unit or IT service providers;

i. ensuring appropriate actions have been done to remediate audit findings of either internal or external auditor, or based on assessment reports of Bank Indonesia;

j. ensuring the adequacy of human resources in either the IT operation/management or the implementation of risk management;

k. if the uppermost official who directly oversees IT is a director, then the aforementioned has the obligation to observe IT budget implementation such as an acquisition of IT and IT training. If the uppermost official is not a director then the monitoring of both said fields can be done by the overseeing director;

l. the director of IT are responsible in the forming and implementation of IT architecture and other strategic plans which affect the Bank's capital significantly, ensuring the organization structure of project management from every IT related project is done in maximum capacity;

m. ensuring that written contracts between the Bank and IT service providers include items regulated in Chapter X – The Use of IT Service Providers.

1.2.2. Information Technology Strategic Plans

Information Technology Strategic Plan are documents which illustrate the visions and missions of a Bank's IT, the strategies which support said visions and missions, and the main principles which become guidelines in the use of IT to fulfill business needs and to support long-term strategic plans of the Bank.

Prior developing IT Strategic Plans, a Bank should carry out analysis regarding related items, amongst others are related data of Corporate Plan, standards and regulations of IT and valid banking industry, technology trends, and results of assessment on current IT environment.

The development of said plans is done by the IT management unit, IT users units and the IT Steering Committee. The documents of IT Strategic Plans include amongst others the following:

a. targets of development of Bank's business;
b. standards of the implemented technology;
c. regulations on which the management are based on (amongst others regarding Bank's confidentiality, security, Products' information transparency and the use of customers' personal information);
d. application requirement plan for new products and activities, and developments of existing products and activities;
e. costs related to the implementation of plans;
f. necessary processes to achieve efficiency;
g. customers service and quality of technology performance;
h. analysis of IT resource capabilities of the Bank;
i. future optimization of IT infrastructure;
j. the ability to adapt and to integrate with new technological advances; and
k. the ability to adapt to Indonesia's atmosphere of macro economic development.

In forming IT Strategic Plan, a Bank should consider the following items:

a. align with the Bank strategic plan in every respect;
b. align with strategies and activities of each business unit, market state, and structure of demography, as well as customer segmentation;
c. a management understanding regarding roles of IT in supporting the operations of Bank's business already existing and in course of planning.
d. a management understanding regarding the relationship between IT resources currently used and planned, with strategy and work plan from IT users unit;
e. direct and indirect benefits against the costs of using technologies;
f. needs of new investments in the field of technology.

1.2.3. Information Technology Organization

1.2.3.1. Functions of IT Risk Management

Banks should have a risk management function on the use of IT in Bank's organization which involved parties having and overseeing risks, as well as carrying out tests and verifications.

Banks should have policies on how identification, measurement and monitoring of risks on every activity/business are carried out periodically by Risk Management Unit collaborating with IT Operation unit and IT users unit. Furthermore, for certain functions such as the function of information security and the function of Business Continuity Plan, the implementation of risks management remains as the responsibility of work teams or officers who run said functions. Therefore Bank's management must ensure adequate monitoring and reports regarding activities related to IT and its risks. For the process of monitoring and reporting to run optimally, internal and external audit should carry out the function of tests and verification in every IT inspection.

To optimally implement risk management of information security, in addition to the IT functions that carry out the daily securities duties required in IT operations, Banks need to have a bank-wide function of information security program management and monitoring. The first function can only carry out the determined procedures and can not make decisions to grant exceptions or to alter the determined standard and procedures. Ideally, Banks need to separate those two functions so that the function of Information Security Officer should not responsible to the IT unit/department but to the directors. In practice, Banks may establish a policy to implement the two functions mentioned above that suit to the organization structure and business complexity, as well as supporting technologies used by the Bank.

1.2.3.2. Organization Structure of IT Unit

Banks should have an organization structure suitable with the requirements of IT management and usage, and at the very least considers the following:

a. organization structure specifically illustrates lines of authority, reporting, responsibilities (and replacements if necessary) for every critical IT functions;

b. segregation of duties is present to prevent an individual having responsibilities on different and critical functions in a way that may result difficulties in detecting errors. For example, personnel responsible for information security administration should be separate from development and IT operations;

c. organization structure which does not allow any opportunity of any individual to perform and/or conceal errors or violations independently in the carrying out of duties, as well as disabling security measures;

d. for relatively small Banks or branch offices in remote areas, where it is not possible to implement adequate segregation of duties (segregation of incompatible duties) either entirely or partially, it must be replaced by another form of monitoring or by compensating controls, to prevent errors on IT operation. In determining the form of said compensating controls, Banks have to consider data Ownership, responsibility on transaction authorization, and data right of access. Compensating controls would include, audit trail, reconciliation, exception reporting, transaction log, supervisory review, independent review. IT management must remain based on prudence, despite the implementation of compensating controls;

e. personnel emplacement through consideration of competency (knowledge and skill) of human resources according to the position (rank);

f. distribution of responsibilities and assignment of goals are well arranged in-between functions of risk management and functional fields of IT management.

1.2.3.3. IT Risk Management of User Units

Chief of IT user unit/department has also the responsibilities on the management and of IT, which are amongst others:

a. ensuring the existence of continuing communication process with IT unit regarding the needs related to Bank's business strategy, such as arrangements to-issue new product;
b. determining and conveying needs of SIM to IT unit;
c. ensuring employees in users unit participate in testing processes done on the application which will be used by said unit;
d. ensuring IT users in said unit abide by the predetermined security procedures.

Ownership of data/information is in the hands of user unit/deparment. IT Operation unit are responsible to the custody of asset in the form of data/information. For that, IT unit must determine standards and procedures of Custody of Corporate Assets to manage said data/information adequately.

1.2.4. Personnel Control

Other than requiring proper choice of technology, Banks also require personnel who possess suitable abilities and skills and capable to support the carrying-out of functions of IT maximally. Therefore Banks need to implement personnel control, amongst others by implementing:

a. issuance of procedures for the recruitment of new employees, relocation and promotion, as well as IT officer dismissal. This procedure is valid for Banks' employees, consultants, honorary employees and service provider employees. For sensitive functions of IT management, a background investigation of candidates in the recruitment process is a must;
b. issuance of duties, responsibilities, expectation/target transparently;
c. issuance of standards for work performance assessment, wage/salary and benefits, as well as retirement funds;
d. Education and training programs as well as performance assessment to preserve and increase the quality of employees of both IT Operations and users.

For such controlling steps to be effective, Banks need to have plans of human resources management integrated with IT Strategic Plan.

1.2.5. Project Management

In the event that Banks carry out important and large-scale IT development and acquisition, an organization in the form of Project Management is required. Such is needed to ensure that the application system that IT unit render to users unit to be used, is well-developed and has accommodated the users' requirements as well as in accordance with Bank's IT system. The team of Project Management administrate each project advances and assist in coordination between project's organizer and potential users of IT system/application on every project, and also report it to the IT Steering Committee. The form of a project management in the Bank's organization is conformed to the complexity and magnitude of the Bank. It possibly will be in the form of a permanent unit or an *ad hoc*.

1.2.6. Management Information System (MIS)

Banks must ensure the existence of an MIS is able to produce the required information in terms of supporting the role and function of management effectively. The MIS must be able to provide the required information completely, accurately, most recently, wholly, securely, correctly, consistently, promptly, relevant, and applicable to ease the process of planning and decision-making which support the efforts to achieve Bank's business strategy.

In addition to that, the MIS possessed by a Bank must be able to:

a. facilitate the management of Bank's business operations including services to customers;
b. record and gather information objectively;
c. distribute data/information to various units according to the type of information, quality and quantity as well as frequency and duration of required report submission;
d. increase the effectiveness and efficiency of Bank's communication;
e. assist the Bank to comply with the law and regulation;
f. support the process of performance assessment of the total units/departments.

Technology advances might increase the availability of information that result IT unit holding an important role in the effectiveness of a Bank's MIS. The IT determines policies, procedures and control of database management, and reports forming to alleviate the assurance of MIS effectivity.

1.2.7. Documentation

Banks' Management must ensure that internal control or audit can perform tests and validation of policies, processes, procedures, standards, and requirements in the management of IT. For that, Banks must possess the documentation of security policies and operational risk management that are clear complete and applicable, especially the ones linked to IT-related risks in each IT users working unit.

1.3. RISK MANAGEMENT RELATED TO INFORMATION TECHNOLOGY

The ability of a Bank to mitigate the IT risks depends on the result of identification, measurement, control, and monitoring of said risks having the potential to jeopardize the Bank's security and operations.

The essential process of IT-related risk management of a Bank consists of four important items, which are:

a. planning the use of IT;
b. assessing IT-related risks;
c. determining the process of measuring and monitoring risks related to the use and the carrying-out of IT;
d. implementation of IT control.

1.3.1. IT Usage Planning

As have been explained above, Banks must possess an Information Technology Strategic Plan that supports Banks' business strategic plan. Furthermore, part of the Information Technology Strategic Plan which would be implemented in the next one year is stated in the Bank's Business Plan (BBP), in Management of Policies and Strategies section. Apart from it, if the BBP contains sections related to the development of new products and activities as well as transition of bank's office network, then it must also be stated in New Products and Activities Development as well as Bank's Office Network Transition sub-chapter. Each plan of expense related to IT Strategic Plan which is going to be implemented in a particular year must be added into the balance projection in the Business Plan.

Considering that IT strategic plan is long term, then to keep the accordance with the Bank's business and IT development, Banks are advised to carry out periodic evaluation which consist of, amongst others, Bank's IT performance as well as the achievement of determined objectives and finance. By doing so, the balance sheet projection in Business Plan will be more realistic and continuous year after year.

1.3.2. Continuous Risk Assessment

The policy of IT management in general has the aim of ensuring that the carrying-out of IT can support the achievement of the Bank's Business Plan and ensuring that risks related to the carrying-out of IT directly or indirectly might be resolved.

In performing the risk identification and risk assessment, the management must previously ensure risk awareness in the Bank's entire corporate is exists, which are:

a. the executives and directors' risk awareness ;
b. a clear understanding regarding risk appetite of the Bank;
c. an understanding on prevailing laws and regulations;

d. transparency and integrity of responsibilities regarding significant risks from each aspect related to IT operation.

To ensure the abovementioned items, the Bank might perform the risk awareness program for all employees and caretakers of the Bank, or perform other methods which is able to increase the awareness of IT users on the of existing risks.

1.3.2.1. Types of Risks Related to Information Technology

Banks must possess an integrated risk management approach for the ability to identify, measure, monitor, and to control risk effectively. Technology-related risks must be reassessed together with other risks to determine Bank's risk profile entirely. As such, the main risks of IT are:

a. Operational Risks

Operational risks are attached to any products and services provided by Banks. The use of IT might result in operational risks brought about by insufficiency/discord of designs, implementation, and response on system or computer and its equipments, security methods, testing and standards of internal audit as well as the use of other party's service in the IT operation.

b. Compliance Risks

Compliance risks might arise if a Bank does not possess systems that capable of ensuring the Bank's compliance to prevailing regulations such as the confidentiality of customer information. Compliance risks can affect the reputation of the Bank outrageously, and also to business opportunities and possibilities of expansion.

c. Legal Risks

Banks face legal risks brought about by lawsuits, the absence of supporting regulations or the inadequacy of legal ties, such as as the negligence of a contract's requirements.

d. Reputation Risks

Negative public opinions might arise because of, amongst others, the failure of a product-supporting system, cases on Bank's products, and the inability of the Bank to sustain customers' service during system downtime. Such negative opinion can decrease Bank's ability to maintain customers' loyalty and the success of Bank's products and services

e. Strategic Risks

This type of risk arises because the divergence of implemented IT with the Bank's strategic goals and the strategic plan in the course of achieving such goals. This is because either the quality of implementation or the resources used on IT are not adequate. Said resources include communication lines, operating systems, delivery network, as well as the capacity and capability of IT management.

1.3.2.2. Risk Assessment

In using technology, the Bank's management must perform strict, total, cautious, and accurate analysis process to identify and quantify risks, as well as to ensure the implementation of Risk Management. Therefore, risk assessment must be carried out in continuity with a cycle which includes at least the following four items:

a. **Ongoing data/documents** collection from IT related activities with the potential to cause or increase risks on either future or current activities including but not limited to:
   1) Critical IT assets, to identify points of access and infringement on the confidential customers' information;
   2) The result of business strategic plan reviews, especially a review on the potential risk assessment;
   3) The result of due dilligence and monitoring on the performance of service providers;
   4) The result of reviews on reports or complains submitted by customers and/or IT users to the Call Center and/or Help Desk*;*
   5) The result of Self Assessment by the entire work units on IT-related control;
   6) Audit findings related to IT operation and usage.

b. **Risk analysis** regarding to the potential impact of each risk, such as from fraud programming, computer viruses, system failure, natural disasters, mistakes on used technologies selection, system development and implementation problems, mistakes on Bank's business development prediction.

c. **Priority Establishment** of control and mitigation steps based on the result of Bank's risk assessment as a total. And so Banks ought to formulate levels of risk based on likelihood and the magnitude of impacts, as well as the feasible risk mitigation to reduce such risk exposure.

d. **Monitoring of control and mitigation activities** has been done on risks identified in the previous risk assessment period, which includes, amongst others, action plans of recovery, accountability and responsibility comprehension, reporting system, quality control including compensating control*.*

1.3.3. Risk Measurement and Monitoring Process

As have been described previously there are several types of risk related to the use of IT, but one with the biggest potential is operational risk. This requires attention considering operational risk is difficult to quantify. Banks need to consider the severity of consequences of identified risk on the condition of the Bank as well as the frequency of the risk. Applicable methods can be quantitative or qualitative depending on complexity of business and the technology used.

In qualitative methods, the severity of consequences and its likelihood are explainable through words or by descriptive rankings. Examples of simple measurement method are, amongst others, using a check list or using a subjective risk rating such as High, Medium, or Low. Bank should establish the criteria for High, Medium, or Low in said risk rating, and implement those consistently. To be capable of providing a more sensitive result of risk assessment, Banks might increase their risk rating method from 3x3 to 4x4 until 10x10. An example of ratings using risk matrix 5x5 is as the following table:

RATE OF OCCURENCE / LIKELIHOOD	**IMPACT/ CONSEQUENCES / LOSS**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	Low	Medium	High	Very high	Very high
Likely	Low	Medium	High	Very high	Very high
Possible	Very low	Low	Medium	High	High
Unlikely	Very low	Very low	Low	Medium	Medium
Rare	Very low	Very low	Low	Low	Medium

There are many application programs of risk measurement using a quantitative method. This method use statistic data regarding the occurrences and consequences. Risks are measured based on rate of occurrence and the severity of consequences/impacts. Some Banks use VAR for risk assessment with quantification method which analyzes database likelihood and consequences from past occurrences.

If Banks use risk management information system package which includes risk measurement application as a tool of the implementation of risk management in the use of IT, Banks must consider the assumptions used in the system, as well as business commonsense and professional diligence.

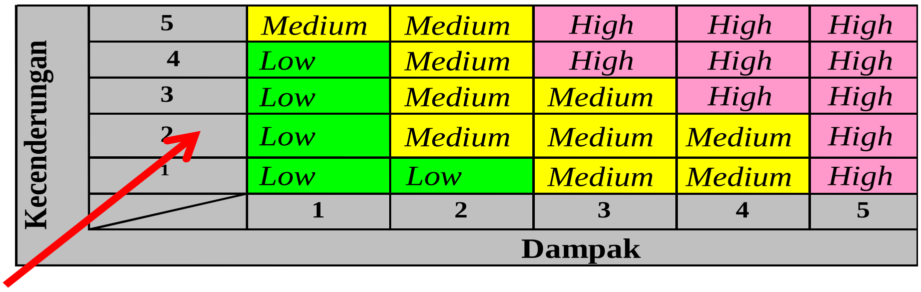
Meant for the risks that have been identified and assessed or measured are able to be monitored by the management, Banks must have a Risk Documentation or what is often mentioned as a Risk Register. An example of constructing the Risk Register is available in Appendix 1.1.Examples of Risk Assessment. Banks might determine components of Risk Register different from the Appendix 1.1. but must include at least the following items:

a. determine assets, processes, products, or occurrences containing risks;
b. measurement or classification of the likelihood of occurrences and impact (Inherent Risk Assessment);
c. potential risk treatmenst such as Accept, Control, Avoid or Transfer (ACAT);
d. measurement or classification of the likelihood of occurrences and consequences after ACAT (Residual Risk Assessment).

In the documentation of the potential risk treatment, Banks must consider, amongst others, risk appetite of the management, facilities functional as preventive control or corrective control, and the accordance of risk mitigation plan with Bank’s financial condition. This risk documentation must be periodically renewed.

Potential risk treatments applicable by a Bank as mentioned in point c above is as the following:

a. The management decides to accept a risk if the severity of the impacts and its likelihood remain in the organization tolerance limit **(Accept)**.
   As an example
   1) By implementing Risk Acceptance Criteria related to the evaluation and risk response, such as Final Risk Value “Low”.



Kecenderungan	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Medium	Medium	High	High
	2	Low	Medium	Medium	Medium	High
	1	Low	Low	Medium	Medium	High
		1	2	3	4	5
		Dampak				

   2) Final Risk Value “Medium” or “High”, but has been decided to be accepted by the management, and a procedure system is prepared to monitor the risk such as by providing additional capital in accordance with the risk potential.

b. The organization decides not to carry out an activity or choose another alternative activity capable of producing equal output to avoid the occurrence of risks (**Avoid risk**).
   As an example is administrator privilege on users using PC which contain risk of the existence of malicious code in the PC. This risk can be avoided by not giving privileges to users so as render them unable to change the configuration and to install software on PC.

c. The organization decides to reduce the impacts or either the likelihood of risks (**Control / Mitigate**).

   As an example is, the use of PC to support organization's business process contains risk of hacking on the PC. Risk Management is carried out by the installation of firewalls to prevent unauthorized access.

d. The organization decides to avert the entire or a part of responsibilities of a process conducting to a third party (**Transfer**).

   As an example is the use of rooms or buildings facilities contains a risk of fire. This risk is dealt with by transferring the risk to an insurance company, that is by insuring said rooms or building facilities.

1.3.4. Implementation of Information Technology Control

The management must implement adequate control practices as a part of IT risk mitigation strategy as a total.

Control practices amongst others are:

a. implementation of policies, procedures, organization structure including its work flow;
b. effective internal control that capable of mitigating risks in IT processes. The scope and quality of internal control are the key in the risk management process, so as for the management has to identify specific requirements of internal control needed in each and every implemented policy and procedure;
c. the management must establish policies and procedures as well as standards (information security management system) required to secure assets related to the IT operation and usage including data or information. Further regulation regarding Security are available in Chapter V – Information Security;
d. the management must evaluate the result of review and test of BCP for every critical operation. Further regulations regarding the BCP are available in Chapter VI – Business Continuity Plan. Identical with management of information security, the BCP is a comprehensive strategy and carried out by the entire work units of a Bank;
e. the management must ensure the existence of policies and procedures regarding the use of third party service providers. The directors must completely understand the risks related to the use of services from service providers for some or all IT operations. For that, IT unit must evaluate the ability of service providers to safeguard levels of security to at least at the same or more secure degree than the one implemented by the internal Bank, either from aspects of confidentiality, of data integrity and of information availability. Stringent observation and monitoring must be conducted because the responsibility of Bank's management is not eliminated or lessened by employing IT operation outsourcing to IT service providers. Further regulations are available in Chapter X - Outsourcing;

f. other than implementing control mentioned above, insurance can be used as a complement to the efforts of mitigating loss potential in the IT management. Risk to be insured is the residual risk. Banks should periodically review requirements, scope of, and covered insurance value.

CHAPTER II
SYSTEM DEVELOPMENT AND ACQUISITION

2.1. INTRODUCTION

System development and acquisition includes suitable management of Information Technology system through the process of identification, development/acquisition, implementation and maintenance of Information Technology used in Bank's business. System development and acquisition can be in the form of internal software developments or software purchases, hardware and system development services from a third party. In a case of weak management and control on the process of system development and acquisition, Banks can face multiple risks from errors, frauds or even unsuitable products or services.

2.2. DUTIES AND RESPONSIBILITIES OF MANAGEMENT

During the process of Information Technology development and acquisition, the management must perform control activities to produce systems and data secure and integrated, as well as supportive in achieving the Bank's goals. Steps which include, amongst others:

a. determine and implement procedures and methodologies of the development and acquisition of Information Technology consistently;
b. implement project management in developing the main application system;
c. ensure the testing done in the time of system development and acquisition is adequate;
d. ensure the system being developed is in accordance with the users' requirements;
e. ensure the accordance of a system with other systems;
f. carry out documentation on developed systems and their maintenance;
g. possess an application change management;
h. adequately identify, measure and control potential risks related to system development and acquisition;
i. Ensure the possession of procedures of system/application development in emergency situation or emergency changes, by the Bank.

2.2.1 Project Management

For developments/acquisitions of the main application system, Banks must possess project management to ensure said application system has been developed with a suitable structure and has accommodate users' requirements, as well as in accordance with the Information Technology system of the Bank. Project management can be in the form of a team of which its members consist of personnel from IT unit and users. Meanwhile an internal audit is an independent party providing recommendations for both work units in ensuring the sufficiency of control on application system (advisory capacity).

2.2.2. Change Management

What is meant by change management is a process of management of an alteration in program development, such as an alteration on user requirement, or an alteration on supporting technology.

The procedure of change management must be arranged, conducted and documented well. Requirements for alteration must be investigated before any agreement, to decide other methods in said alteration, cost of alteration, as well as necessary duration for programming activities. The real reason of alteration must be properly recognized and documented. Audit trails from every requested alteration must be maintained. Programmer activities must be organized and observed, and all duties must be observed thoroughly over the deadline.

2.3. POLICIES AND PROCEDURES

Issues of concern in policies and procedures of development and acquisition are, amongst others:

a. Minimum including the following items:
   1) identification and analysis of user requirements;
   2) definition of requirements (user requirement);
   3) System planning;
   4) programming;
   5) testing;
   6) implementation;
   7) post implementation review*;*
   8) Maintenance.

b. Each and every development and acquisition of Information Technology system must be under the Information Technology work unit control.

c. For applications developed by a vendor or established by a third party, Banks must carry out a selection process of a vendor/third party referring to BI's guidelines regarding outsourcing as well as policies and internal procedures. Banks must also ensure the adequate trainings and manuals are provided as a part of the contract between the Bank and the vendor.

d. Policies and procedures required in project management are, amongst others:
   1) Feasibility study is necessary to know the cost and benefit from a system development, as well as to determine whether to utilize internal resources or outsourced;
   2) Relevant security prerequisites must be clearly specified before new systems are developed or obtained. Said security prerequisites must be in accordance with the architecture of information security of the Bank as a total;
   3) Proper planning are necessary to ensure the project achieve its objectives;

4) Banks must carry out segregation of environment for developments, testing and production, including access restriction to each environment;
5) If the system is supported or maintained by vendors/other parties, proper analysis for software selection are necessary to ensure that users and business requirements have been accomodated;
6) Contract agreements between Banks and vendors must be legally bound;
7) Banks must implement maintenance management for every implemented process of system development and acquisition;
8) All results (deliverables) on every phase of project management must be well documented.
9) Banks must possess formal project plans which include the following items:
   a) identification of project, sponsor, and project manager;
   b) project objectives, background information and development strategies;
   c) description of the main responsibility of every personnel in the project management;
   d) procedures to gather and distribute information;
   e) criteria of targeted results for each phase of development (acceptance criteria);
   f) security and control problems in consideration;
   g) procedures to ensure that the manager assess, observe, and arrange internal and external risks appropriately along the development cycle;
   h) cut off date to divert the use of a previous application system to the most recent version of the result;
   i) standards of development that are going to be used for project monitoring, system control and quality assurance;
   j) types and levels of documentation produced by related personnel in every phase of the project;
   k) phase schedule of the project and activities to be finished in each phase;
   l) estimation of initial budget of the entire cost of the project;
   m) testing plan which identifies the testing requirements, and a schedule of testing procedures;
   n) training plan which identifies the training requirements, and a schedule to enable employees is capable of using and maintaining post-implementation application.

e. Policies and procedures of change management required for a Bank are modification procedures which include at least:

1) review before modification and authorization;
2) testing before modification (in a separate testing environment);
3) data backup and source code procedure before modification;
4) documentation which consist of:
    a) Explanations on modification;
    b) Reasons of an implementation or a refusal on suggested modification;
    c) Names of individuals who make the modification;
    d) Copies of altered source code;
    e) Dates and times of modification done; and
5) evaluation after modification.

f. Necessary documentation during the process of modification consists of:
1) information;
2) identification of systems, database and affected work units;
3) names of individuals responsible in making alterations;
4) resources requirements;
5) estimate cost;
6) estimate date of completion;
7) estimate date of implementation;
8) consideration of security and capability potential;
9) testing requirements;
10) implementation procedures;
11) estimation of downtime on implementation;
12) backup procedures;
13) documentation updates (program plans and scripts, network topology, user manual, contingency plan, etc);
14) documentation of modification approval from every related work unit (user, technology, quality assurance, security, audit, etc); and
15) documentation of post-implementation audit (comparison between expectation and result).

2.4. DEVELOPMENT AND ACQUISITION RISK MANAGEMENT

Bank’s management is responsible over the risk management of every activity related to development and acquisition of Information Technology system.

2.4.1. Identification of Types of Risk Related to Development and Acquisition

The process of development and acquisition of Information Technology system by Banks can contribute to some risks, which are:

a. Operational Risk

Errors, specification insufficiency, weakness in the developed or purchased system can cause operational risk, amongst others the occurrence of fraud, error and discrepancies on requirements. Such operational risk can also affect other risks such as market, liquidity, strategic and reputation risk.

b. Reputation Risk
   Errors, lateness or mistakes in the development of Information Technology systems, should it ever disturb service to customers, can significantly affect the reputation of the Bank.

c. Strategic Risk
   Failure on a developed system can result in data and information which cause mistakes on decision making by the management.

d. Compliance Risk
   Failure in developments or acquisitions of Information Technology system to follow an alteration on regulations can increase compliance risk for the Bank.

When developments are going to be carried out, the Management must consider the risk related to the following factors:

a. the scope of the system includes the sensitivity of accessed data, protected or controlled, volume of transaction, and the importance level of said activities and functions to the Bank's business;
b. concerning the technology used, includes reliability, security, availability, and timeliness, as well as the ability to follow the developments of technology and alterations on regulations.

2.4.2. Risk Management on Application System Development

In carrying out developments, Banks must determine the methodology to be used. One of the methodologies that can be refered to by a Bank is System Development Life Cycle (SDLC). In SDLC, the development phase of an application system is divided into initiation, planning, requirements defining, design, programming, testing, implementation, post-implementation review, and maintenance. Examples of other development methodologies are such as agile software development, Rapid Application Development (RAD), and other methods which have become a standardization of system development. However, at least in the carrying-out of development with other methods, Banks refer to the phases in this guideline.

2.4.2.1. Initiation and Planning Phase

The initiation phase begins with requirements identification to add, complete or restore a system requested by users through a proposal. This initiation phase consists of, amongst others, the following steps:

a. arrangement of proposal with the content of identification of requirements to add, complete or restore a system, purpose and expected benefits, as well as how the system can support business strategy;
b. proposal evaluation by the management;
c. approval on new principles of system development/acquisition or system alteration;
d. feasibility studies which are, amongst others, business consideration, functional requirements, factors affecting the project, and cost and benefit analysis;
e. management approval on feasibility study documents;
f. signing of documents of feasibility study by all related parties.

After the approval of development in the initiation phase, Banks carry out planning to identify in detail specific activities and necessary resources for completing the project. This planning phase produces a project plan that becomes the reference for carrying out the project and must be updated according to the project development.

2.4.2.2. User Requirement Definition Phase

Based on the document of feasibility study approved by the management, the project management can form a team to arrange requirement definitions in detail as a base of the beginning of application system development. In this phase, every user requirement are gathered based on document/form examples, process specification and existing system, interview with the end user and research as well as analysis on valid regulations. This user requirement definition phase consists of:

a. Requirements Elicitation, as an information gathering process regarding the purpose of system development, output/results desired, how the system will accommodate business process requirements and how the system will be used.
b. Requirements Analysis as the process of understanding problems and requirements to determine possible solution. In this phase, general estimation is determined from development duration and cost of every requirement. The result of requirement analysis is used to produce business process flows (such as Use Cases Modeling and Data Flow Diagrams) which can explain the understanding of the requirement and its solution, for both users and developers.
c. Requirements Specification as the process which describes functions of the system which is to be developed, from both of the software side and supporting hardware as well as database design. Requirement specification must be complete, comprehensive, able to be tested, consistent, clear and detailing requirements of necessary input, process and output.
d. Requirements Management as the process to identify, controls, and store every alteration of requirements during development.

2.4.2.3. System Planning (Design) Phase

This phase converts information requirement, identified functions and networks during the initiation phase and planning, into design specification which is to be used by developers. One of the design technique is by using prototype which develops scaled models of the design from a part of application such as monitoring display, data structure and system architecture. End users, designers, developers, database administrator and network administrator must review choosed prototyped designs in an iterative process (repetitive) until decided what design is to be used. Personnel of auditor, security and quality assurance must be involved in the abovementioned process of review and approval.

In the design phase, an application control standard which includes policies and procedures related to user activities and integrated control in the system which is to be developed, is required. In this phase, internal audit participates in giving suggestions on control that must be implemented in the application system. This phase is required to increase security, integrity and system ability by ensuring authorized, complete, and secure information of input, process and output.

Based on the purpose, control is divided into preventive control, detection/findings, or correction. Control to be conducted should include at least:

a. Input Control

As a minimum can include checking of data validity, data range / parameter, duplication of input data;

b. Process Control

Ensuring processes to work accurately and can store or reject information. Process control which can be done automatically by the system includes at least Error Reporting, Transaction Log, sequence checking, and backup file;

c. Output Control

Ensuring the system to manage information securely and to distribute information from the result of a process accurately as well as to delete information which has gone past retention.

2.4.2.4. Programming Phase

In this phase the design specification is converted to an applicable program. During this phase, the Bank must arrange several testing plans. In addition, the Bank must also update the migration plan, implementation and end user training, operator and documentation of maintenance manual.

a. Standards of Programming

In the standards of programming are explained, amongst others, the responsibilities of application programmer and system programmer. The project manager must understand entirely regarding the process of programming to ensure that the responsibilities of the programmer are in accordance, by, amongst others:

1) Restricting programmers' access to data, programs, utilities and systems outside his/her responsibility. Librarian control can be used to manage said access.
2) Version control is a method which systematically stores the chronology of completed copies of programs as well as becoming one of the program documentation.

b. Documentation

1) Banks must manage and maintain detailed documentation for every application system self-developed or products/software bought or developed by other parties, of which said documentation includes:
   a) detailed description of application;
   b) documentation of programming;
   c) forms used (database, displays, and information);
   d) naming standard;
   e) Guidelines for operator and for end users.
2) Documentation must be capable of identifying development standard, such as system narration, system flow, system exclusive coding, and internal control on said application documentation itself.
3) In the case where products/software are bought or developed by other parties, the management must ensure that a review has been done, internally or by independent parties, on how said products/software are in accordance with the Bank's documentation minimum standard.

2.4.2.5. Testing Phase

Banks must carry out several series of testing to ensure the accuracy and if the application system is functioning according to the user requirements, as well as the connection of the application system with other application systems (interoperability) of the Bank. Every correction and modification during the testing must be documented to safeguard the integrity of program documentation entirety. Banks must complete the guidelines for users and organizers as well as prepare implementation and training plans. Testing by Banks include, amongst others:

a. Unit Testing,
b. System Integration Testing,
c. Stress Testing,
d. User Acceptance Test.

User Acceptance Test (UAT) is a final test by end users on the developed system/application to ensure that the functionality of the entire system is in accordance with user requirements on user requirement definition, before finally deciding to proceed to implementation. In this phase, internal audit can participate on testing as well, given that they remain keeping the level of independency if said internal audit needs to ensure availability, sufficiency and effectiveness of control in the system. If the result of the test proves that the system/application is in accordance with user requirements, then there must be a UAT event report approved by users.

2.4.2.6. Implementation Phase

In this phase, the main issues required are, amongst others, implementation schedule notification, training on users, and installation of approved application system into the production environment. Other important issues to be concerned are, amongst others:

a. review of program integrity in a form of adequate internal control over conversion of source code into object code which is going to be implemented;
b. migration of data from the old system to a new system;
c. review of accuracy and security of data from the result of migration to the new system;
d. the possibility of parallel runs between the old system and the new system, until it is ensured that the data in the new system are accurate and reliable;
e. data integrity, whereas Banks must ensure the accuracy and reliability of database and data integrity;
f. during implementation, patching data can greatly affect data integrity on database in the production server, and so must be avoided;
g. regulations of source code and database archiving from the old system.

2.4.2.7. Post Implementation Review

The management must carry out a post implementation review at the end of a project, to acknowledge that the entire activity in the project is done and the objectives of the project are achieved.

The management must analyze the effectiveness of project management activities by comparing cost plans and realizations, benefits gained, and timeliness of the project schedule. The result of the analysis must be documented and reported to the management.

2.4.2.8. Maintenance Phase

Hardware, software and documentation must be maintained to ensure the effectiveness of system operations. Banks must determine the methodology of maintenance suitable with the characteristics and risks of each project, from existing application system.

2.4.2.9. Disposal Phase

Every developed software which is no longer be used in operational activities, and based on considerations of the management that said software will no longer be required or maintained, and then said software will be on the final phase in SDLC which is disposal/termination phase. Such are done to ensure the system used in operational activities is the most accurate and most recent, as well as avoiding misuses by unauthorized parties. Further regulation regarding policy of disposal is explained in Chapter III Operational.

2.4.3. Risk Management on Acquisition

In the case of using an application system purchased from third party (acquisition), then it needs consideration on the accordance of said system specification with the requirements, its effect to existing systems, post sales technical support, company's financial condition, documentation comprehensiveness, escrow agreement and training. Identical with developing its own application system, a feasibility study of the acquisition project must be formalized by the management approval, must have a user requirement definition, mush have adequate security control, and there are tests and product implementation. The same process is also implemented in the acquisition of hardware and other software.

Banks must develop criteria of vendor selection, and review on the vendor's capability, related to, amongst others, financial condition, support level, and security control, before deciding the choice of products or services from vendors. Banks must consider related regulations and guidelines of Bank Indonesia regarding outsourcing, as well as the Bank's internal regulation. In addition, Banks must review contracts and licensing agreements to ensure the rights and responsibilities of each party are clear and reasonable. The Bank's legal advisor must verify that the performance guarantees, access to source code, copyright issues, and security of software/data are arranged clearly before the management signs the contract.

2.4.3.1. Acquisition Standard

Acquisition standard must be implemented to ensure that the purchased product has met the functional requirements, security criteria, and reliability. The main tool in managing the Acquisition project is a request for proposal (RFP) which includes at least functional requirements, security, and operational requirements accurately, clear and detailed. In a Acquisition system, the project manager must carry out, amongst others:

a. Global review regarding the accordance of vendors, contracts, licenses and products, to the existing system.
b. Compare the offer with the prerequisites in a project, and with other offers.
c. Review the financial condition of the vendor and its commitment to service.

d. Obtain suggestions from a legal advisor before the contract is signed by the management.

2.4.3.2. Acquisition Project Guidelines

Concerns in Acquisition project are, amongst others:

a. Acquisition project begins with the proposal of plans for a project to the management.
b. Procedures must be formalized to facilitate request process and to ensure the management systematically reviews every request.
c. Requests must be based on Bank’s business requirements, to :
   1) obtain a product;
   2) identify desired system features; and
   3) Illustrate the requirement of information, network interface, software, and hardware components.
d. Banks must arrange a feasibility study to determine whether they need a Acquisition of software which is modifiable according to the requirements or off-the-shelf.
e. Approval from all involved parties on said feasibility study must be documented to further be a base of making a Requirement Definition, as have previously been mentioned in sub section 2.3.2.2 above.
f. Following an acceptance of an offer, Banks must analyze and compare the offers among participants on determined requirements. Vendor proposal must discuss clearly all of the Bank’s requirements and identify other issues which can be implemented.
g. Banks must have procedures to ensure that the review on offers is done correctly. The selection process will produce potential vendor list.
h. The management must assess the financial condition’s stability and the commitment to service of selected vendor.
i. Banks determine the product and the vendor as well as negotiate the contract. In this case a legal advisor should review said contract before its approval.

2.4.3.3. Escrow Agreement

In the case where the center application is made by another party (vendor) and the source code is not given, Bank’s interest of safeguarding business continuity must be protected. To mitigate risks of vendor’s support being discontinued, Banks must consider the need of having a written agreement in the form of escrow agreement on software considered important. Items to consider in the use of escrow agreement are, amongst others, vendor reputation, indicated by how the software are used by various parties in and out of the state.

In escrow agreement, an independent third party should be assigned to store the source code. Banks must periodically (per year minimum) ensure said third party stores the most recent version of the source code. The selected storing agent must ensure the number and date of stored source, and ensure the integrity of said source code to the vendor.

2.4.3.4 . Development Contract and License Agreement of Software

a. Software License - General

Banks must ensure that in the license are, amongst others:

1) written clearly whether the use of said software is exclusive or not;
2) included who and how many personnel are able to use the software, including the use in a network;
3) included whether there are limitation on the usage location;
4) included whether the Bank requires a license of location for users which is not limited to a certain location, it must be ensured that said item are available in the contract;
5) included whether the Bank wants other related entities to use said software, such as subsidiary or vendor, must be included in the license list.

Banks must ensure that the license is also valid for the back-up copy of all important software which are required at a remote site in the carrying-out of disaster recovery, or ensure the continuity of Bank's business (business continuity plan). Banks must understand clearly regarding the license duration, and if they want the license continuously to use software, it must be ensured that said intention is explicitly written in the contract.

b. Standard of Development Specification and Software Performance

In the Acquisition of software, Banks must make an agreement contract with development service providers which include the standard of program specification which is expected to be in accordance with user requirements, amongst others:

1) expected performance and software functions;
2) equipment prerequisites and necessary infrastructure to run said equipment;
3) functional identification and specification where operational software works, and milestone identification of functions which are necessarily done by the vendor during the development process;
4) arrangement of modification permit from specifications and standards of performance during development process;
5) identification of test requirements to determine the accomplishment of software performance standard;
6) actions to be carried out by developers if the software fails during tests.

c. **Maintenance**

Banks must consider if the license agreement or development has included the agreement regarding issues necessary for maintaining software such as documentation, modification, updates and conversions. The agreement includes, amongst others:

1) vendor provides software documentation, including documentation of application system and usage technical guide;
2) the implementation and cost of updates and modification of software;
3) the possibility of the Bank accessing the source code if service providers no longer offer their service or if there are modifications which can not be done by service providers;
4) The possibility of software and data conversion to a different one in the future.

If necessary, the issues above can be included in a separate maintenance agreement.

d. **Warranty**

Further inquiries are necessary for Banks to do to ascertain that software license from a vendor guarantees that the software:

1) does not violate the intellectual property rights from other parties across the world
2) does not include unexpressed secret/restricted code or automatic restriction in the agreement
3) will perform according to the specifications, and the vendor's responsibility if problems occur must be stated
4) guaranteed maintenance within the agreed duration
5) License agreement remains valid in the event of merger, acquisition or ownership alteration of either Bank or vendor.

e. **Dispute Resolution**

Banks must insert clauses on dispute handling in the contract and license agreement. An understanding regarding said clause will increase the capability of the Bank to solve problems through the best possible way and enable the Bank to continue the software development during the resolution of conflicts.

f. **Agreement Modifications**

Banks must ensure that software license clearly states that vendors cannot modify agreements without written signatures from both parties involved.

g. **Security**

Banks must determine the criteria of security control on Information Technology system which is to be the performance standard of security features in the license agreement and software development agreement. Said standard must ensure that the developed software is consistent with the entire security program in the Bank. Said license and development agreement must discuss:

1) Continuous responsibility from vendor to safeguard the security and confidentiality of Bank's resources and data.
2) Prohibition on vendor to use or disclose Bank's information without approval/consent of the Bank.
3) Vendor guarantee that the software does not contain a back door that enables unauthorized access to Bank's data and application system.
4) Explicitly state that vendor will not use features of software that cause said software not to function properly.

h. **Sub Contract to Other Vendor**

Banks must determine a clause in the development agreement which prohibit vendor reassigning the contract to a third party without the Bank's approval. If there are conditions where parts of the development of equipment have to be subcontracted then it must be with the Bank's written approval. In approving said sub contract agreement, the Bank must consider the level of difficulty and availability of experts of the software development as well as Bank's data security. Apart from that, the Bank must ensure that there is a clause stating the vendor is responsible on the software even if it is assembled or developed by another party.

2.4.4. Risk Management on Application System Maintenance

Maintenance activities including routine services and modifications on hardware, software, and related information, should be done to ensure the effectiveness of the use of Bank's Information Technology. For this reason is needed Standard Operational Procedures regarding change management to ensure that the alteration during maintenance phase will not disrupt Bank's Information Technology operation or decrease the performance/security of the system. Change management includes entire modification, minor modification, and emergency modification.

2.4.4.1. Change Management

Management must determine the change management SOP in detail which contains procedure of authorization, testing, documentation, implementation and socialization on the technology modification.

Modification includes hardware and software. Hardware modifications are needed to replace old or useless equipment or even to increase performance or storage capacity. Software modifications are needed to achieve the user's requirements, to repair software problems and security weakness or to implement new technology. Banks must coordinate the modification of software and patch through the process of centralized change management because of the relation between application system and operational system.

Based on its rating of importance, modification is categorized to:

1) Major modification, is a significant functional change on the application system which is caused by conversions or development of a new system due to mergers or acquisition involving the Bank. Major modification must be implemented according to a structured process such as the one in the cycle of system/application development.
2) Minor modification, is the carrying-out of changes on the application system or operation system software to increase performance, handle problems or increase security. Minor modification standard must include alteration requests, reviews and agreement procedures as well as requisitioning the management to plan, to test and to document every alteration before its implementation. Banks must review all suggested modifications to ensure the accordance of the modifications with existing systems and ensure that only approved modifications are implemented. Banks must determine the standard of programs agreement which include procedures to verify the result of tests, examine altered codes and to ensure the accordance of source code. After the program modifications are finished, all source code must be secured in the library of both the most recent version and the altered version.
3) Emergency modification, needed to handle problems on software or to quickly recover operational process. Although such modification must be completed quickly, it must be implemented and controlled well. As what is proper as a modification, emergency modification must be tested before implementation. But if testing can not be done entirely before any implementation, then there must be a procedure to carry out backup file correctly. Such is important to enable the Bank to cancel the modification if said modification causes disruption on the system.

2.4.4.2. Patch Management

Vendor routinely develops and produces patches to handle problems of software, to improve performance, and to increase security. If there is a new patch, Banks must technically evaluate the effects from said patch installation on business and security. Banks must possess procedures to identify the availability of patches from a reliable source. The standard of patch regulation must include the procedure of identification, evaluation, agreements, testing, installations, and documentation of patches. Banks must review every security settings and configuration parameter after the use of a new patch to ensure that the setting has adhered to approved policies and procedures.

2.4.4.3. Library

To ensure the availability of the program used, Banks must possess a Library to store programs. Aside from that also required to be stored are information and/or documents in the form of data and programs related to production server/machine from development and/or testing. Further regulations regarding control of library are explained in Chapter III - Operational.

2.4.4.4. Conversion

In the event of a merger between Banks or acquisition that requires an integration of the system used by the Banks involved in the merger or acquisition, then conversions are needed. In this process, major modifications are done on the existing application system or operation system and new system developments if necessary. In this conversion process, a structured process such as the cycle of system/application development must remain implemented.

Considering the complexity of the system in each Bank involved in a merger, a comprehensive analysis on the effects of conversion on Bank's operations is needed, especially on transaction processing. So that the conversion runs effectively, Banks must anticipate an increase of request of balancing, reconcilement, exception handling, users and customers support (help desk), troubleshooting, network connection, and administration system.

2.4.4.5. Documentation Maintenance

A standard of documentation must identify the approved primary documents and detail documents and in a suitable form. The documentation must contain every change to system, application and configuration according to the predetermined standard.

CHAPTER III
INFORMATION TECHNOLOGY OPERATIONAL ACTIVITIES

3.1. INTRODUCTION

The development of Information Technology (IT) enables Banks to carry out more and more complex operations. IT operations are not only concentrated on Data Center but also to other activities related to the use of integrated application, various communication media, internet connections, and various computer platforms. Meanwhile access of input and output can be done by many users from various locations. Also the same with processing, it can be done on various locations far-off but connected, by online real-time, on-line, or even off-line. And so is required an adequate control on IT operations for the Bank to minimize the risk of disruption of confidentiality, integrity, and availability of information.

This chapter discusses the activities, risks, and control of IT operations that can become guidelines for Banks in implementing risk management in the use of IT. Adequate regulation on IT operation is very important to ensure the information in the computer system are complete, accurate, recent, guarded in its integrity, and reliable, as well as protected from errors, frauds, manipulation, abuse/misuse, and damage on data.

3.2. MANAGEMENT OBLIGATIONS AND RESPONSIBILITIES

Bank's management are responsible in ensuring that the whole mechanism of IT operations carried out by in-house or third party are stable, secure, and efficient. The management must establish policies, standards, and procedures of IT operations which guarantee the continuity of Bank's IT operations and ensure its implementation to both IT Operation Department, service providers, or IT user. Errors or failures on IT operations may disrupt operations activities and Bank's service to customers which then affect Bank's reputation. Therefore the management must ensure periodic risk assessment on IT operations and decide proper potential risk management according to predetermined risk appetite.

3.3. POLICIES AND PROCEDURES

Banks must possess a policy which include every aspect of IT operation. The depth and content of said policy are adjusted to the complexity of Bank's IT operations. The policy must be further elaborated in a written procedure used in the carrying-out of IT operations. The procedure contains responsibility, accountability, authorization, guidelines for the people involved. Beside that the management must determine a standard, which is the prerequisites for software and hardware to be used in the environment of production, testing, and development in the carrying-out of IT environments.

3.3.1. Policy of Data Center Operation

Policies, systems and procedures as well as standards implemented in Data Center operations include the activities of running routine or non-routine jobs. Activities related to Data Center operations are, amongst others:

a. job scheduling:
Banks must possess and carry out the schedule of every job in IT operation Data Center effectively and secure from any unauthorized alterations.

b. job operation:
authorization of command line access to IT operators must be restricted according to their authority on predetermined job operation function.

c. distribution of report/output:
The result of information produced by the system (output), in the form of softcopy or hardcopy, might be sensitive or confidential information. Procedure that should be owned by Banks includes determining information to be produced, distribution of output physically or logically and deletion of useless output. Said procedure is needed to avoid the possibility of a disclosure of confidential information and an increase of costs resulted by unnecessary output, and to be able to ensure the security of output*.*

d. the process of backup on-site or off-site, restore, download and upload to data/database*;*

e. activation of audit trail.

3.3.2. Policy of Capacity Planning

Banks need to possess policies and procedures of capacity planning to be able to ensure that hardware and software are in accordance with business operational requirements and to anticipate the development of Bank's business. Without proper capacity planning, Banks may face the risk of shortage or even waste of IT resources. Capacity planning should be arranged for sufficiently long period of time and always be updated to accommodate existing alterations.

3.3.3. Policy of Hardware and Software Configuration Management

Banks must determine procedures related to:

a. Installation process of hardware and software;

b. Parameter setting (hardening) of hardware and software;

c. Inventory and information updates of hardware and software, network equipments, storage media and other supporting equipments in Data Center.

Inventorizing includes the following:

a. hardware:

hardware inventorizing must be done entirely including taking inventory of third party's hardware that is within the Bank. Important information are amongst others, the name of vendor and models, date of purchase and installation, processor capacity, main memory, storage capacity, operating system, functions, and locations.

b. software:

Banks must inventorize information regarding names and types of software (operating system, application system, or utility system). Other information which must be included in inventorizing of software consist of the name of the maker or vendor, date of installation, version and release number, software owner, parameter setting and active services, quantity of licenses owned, number of installations and the number of users.

c. network equipments:

network infrastructure is important for Bank's operations, so the management must create complete documentation of network configuration. Information that must be included are, amongst others:

1) network diagram;
2) identification of every connection of Bank's internal and external;
3) lists and capacities of network equipments such as switch, router, hub, gateway, firewall, etc;
4) identification of telecommunication vendor providing connection within Bank's internal, between Banks and other parties, and with the internet;
5) plans of expansion and network configuration changes;
6) illustration of network security system.

d. storage media:

information needed in the inventorizing of storage media are, amongst others, types and capacity, on-site or off-site storage location, types and classification of stored data, source system as well as backup frequency and retention period.

e. Data Center supporting equipment

Banks must perform inventorizing of Data Center supporting equipment which include, amongst others, UPS and power control, fire detection and extinguisher, air conditioning, and temperature and air humidity measurement.

3.3.4. Policy of Hardware and Software Maintenance

3.3.4.1. Maintenance of Hardware and Data Center Facility

Periodic preventive maintenance on IT equipments is needed to minimize malfunctions on said equipments and to detect early potential problem. Therefore, Banks need to possess maintenance contract with vendors to ensure the availability of maintenance supports from the vendor. Maintenance should be done according to a predetermined schedule, documented, and reviewed periodically.

3.3.4.2. Physical Security and Control of Data Center Environment

a. Control of Physical Access to Data Center:

   Physical access to Data Center must be restricted and controlled properly. Access door to the Data Center must always be locked, equipped with access card and/or biometric devices. Data Center must not be labeled or provided with a signing board so as to be easily recognizable. Banks must possess a log-book to record visitors of Data Center.

b. Control of Data Center Environment:

   The condition of IT processing environment which is not in accordance with the standard can cause disturbance to IT operations. And so, the management must:

   1) review and assess environment factors of data center, which include, amongst others: power supply, fire, water, temperature, air humidity. Possible environment control can be, amongst others: the use of UPS (Uninterruptible Power Supply), raised floor, temperature and humidity regulation (AC, thermometer, and hydrometer), smoke/fire/heat detector, fire suppression system, and CCTV camera.
   2) ensure the availability of sufficient and stable power supply, and the availability of alternative supply in anticipating a non-functioning main power supply. To anticipate the possibility of a power failure, banks need to ensure power voltage regulator, UPS and power generator can work properly. Banks must also use automatic switching in the event of failure on one of the power supply to maintain power according to equipments requirements.
   3) ensure that the Data Center is equipped with fire and smoke detectors as well as water drain pipes. Furthermore, Banks must provide adequate fire suppression system, automatic or manual. The substance of fire extinguisher and the system must consider the safety of equipments and people inside the Data Center.
   4) use a raised floor to secure the cable system and to avoid the effects of grounding in the Data Center.

c. Performance of Hardware and Software:

Monitoring on hardware and software are done daily as a minimum to ensure that all equipment are operating as they should, such as whether servers remain on/active, the capacity of database and server utility does not go over the limit, and supporting facilities function properly.

3.3.5. Policy of Change Management

Change Management is a procedure which controls additions, alterations, or deletion of objects in a production environment. Said objects can be in the form of data, programs, menus, applications, computer equipments, network equipments, and processes. Banks must possess policies and procedures of Change Management which at least include requests, analysis, and agreement on changes and installation of changes including transfer of hardware and software from testing environments to production environments.

Change Management must consider the following:

a. Change Management Control:

Dependency between application systems used by various units in the bank requires an integrated implementation of IT. Therefore, every change/modification must go through the function of monitoring in Change Management, coordinated and involves representative from user department, IT Operation, information security, and internal audit. The procedure of installation of the change must consider operations continuity in the production environment, monitoring process, and information system security management. The minimum baseline standard must include risks, tests, authorizations and agreements, time of implementation, post-installation validation, and back-out or recovery.

b. Patch Management:

In Change Management, Banks must possess complete documentation regarding patch installation. In addition, Banks must ensure the use of software version of the latest release and most suitable. Banks must also possess the most recent information regarding product repairs, security problems, patch or upgrade, or other problems, which are suitable to the version of software used.

c. Data migration:

Data migration occurs in the event of major changes on Bank's application system, or data merger from several different systems. Banks must possess policies and procedures regarding the data migration. Stages necessary in carrying out data migration begin with strategic plan, project management, Change Management, testing, contingency plan, back-up, vendor management, and post implementation review.

3.3.6. Policies on Problem Response

Without proper problem/incident response procedures, Banks can face financial, operational, and reputation risk from occurring problems. The procedure of problem response must include hardware, operation system, application system, network equipment, and security tools. Further explanation is available in Chapter V Information Security – Incident Response on Information Security.

Banks must maintain necessary tools in handling problems, which are, amongst others:

a. Help Desk

The help desk function is a necessity for Banks to allow quick response on problems faced by users, and to handle them immediately. Banks will face risks in the absence of adequate helpdesk procedure, that is, the inability to ensure a place for users to ask questions and find answers and solutions on their problems. Items to be considered on the function of helpdesk are:

1) a complete documentation of problems is available.

Problem documentation must include user's data, description of problems, effects on the systems (platform, application or others), priority code, current resolution status, parties responsible on the resolution, source of problems (if identified), targeted time to resolve, user contacts, and other relevant information.

2) Knowledge-based helpdesk system.

Banks need to use knowledge-based systems to support helpdesk staff regarding alternative solutions for common problems. Banks should periodically update said system with information from vendors and the experience of helpdesk staff.

b. the use of Power User

Power users are user IDs with extensive authorization. In problem handling, Banks must determine the procedure of use of power user to avoid its misuse. Said procedure regulates the following:

1) decision on who has possession of power user access including the implementation of dual custody password (distribution of password to more than 1 person);
2) a procedure of power user password storage;
3) a procedure of breaking (use) of power user ID on emergency situation;
4) a procedure of power user password changes after being used;
5) documentation of the use of power user in the form of event report.

3.3.7. Policy of Data Warehouse Management (DWH)

Banks must possess policies and procedures regarding control on DWH. The control on the system used for DWH is basically the same as the control implemented on core banking system and other systems as the data sources of DWH. If on the system of source application, said data are treated as confidential and with restricted access, then on the DWH must also be treated as such. This access restriction is not limited on logical access but also to physical access on DWH supporting facilities and the resulting reports. As it is, what is meant by the system includes operating systems, application systems, and network systems.

3.3.8. Policy of Database Management

Failure in managing and securing database properly can cause changes, destruction, or disclosure of sensitive data by users either in purpose or accidentally, or by other unauthorized parties. Disclosure without authorization of confidential information can cause reputation, legal, and operation risks and further cause financial loss. Banks need to have sensitivity classification on information stored in a database, as the base for monitoring. The database storing confidential information requires tighter control than a database storing insensitive information. And so, Banks must possess the function of Database Administrator (DBA) which is responsible on the management of a bank’s database.

Procedures which are obligatory for a Bank related to database are procedures of access, maintenance, problems handling, and administration of database.

3.3.9. Policy of Exchange of Information Control

Transmission of information online or through storage media (such as tape and disk) must be adequately managed to avoid risks related to information security. Banks must possess procedures of information transmission management physically and logically, which are amongst others:

a. Requests and providing of information by internal and external parties;
b. Information transmission through various media, such as: hardcopy, tape, disk, e-mail, post, and internet.

In large banks with high IT complexity, the management must consider the separation of WAN and LAN segment with security equipments (such as firewall) which limit access and data traffic.

3.3.10. Policy of Library Function

The librarian function is responsible for identifying and storing all software and all data stored in various media, such as tape and disk. Beside that librarian also stores copies of every policy and procedure such as Data Center run book manual.

Procedures to be determined are, amongst other:

a. access control to data in the library;
b. handling of data storage media (for data/database and audit journal);
c. retention period of data storage media;
d. testing of data storage media;
e. entries and exits of data storage media to and from the library;

In making policies and procedures as well as standards for the library, Banks must consider the sufficiency of procedures of media storage/back-up and disposal. Data or program back-up must always be updated for a Bank to ensure its ability to restore systems, application, and data in the event of disaster or other disturbances.

3.3.11. Policy of Quality Assurance Function (QA)

Every development and alteration of a system must be through the approval of QA before being moved (migrated) to production environment, in accordance with the guidelines of system development and change management. The function of QA is to assess the quality of hardware and software in accordance with the agreed standards.

3.3.12. Policy of Management of Relation with Service Provider

If the IT used by a Bank is carried out by third party then the Bank must periodically monitor and evaluate the reliability of the service provider related to performance, reputation, or the continuity of service. Therefore, the Bank must assign personnel with the obligation to monitor the services of IT service provider, by using the procedure which at least includes service surveillance, problem report and documentation related to service delivery of the service provider.

3.3.13. Policy of Hardware and Software Disposal

Disposal includes software, hardware, and unusable data or data in which period of retention has ended. Old versions of source code no longer used must be stored with clear indication of dates, times and other information when it is replaced by the newest version source code. The necessary actions are, amongst others:

a. moving data from production system to backup media by using mechanism in accordance with procedures, including testing and backup procedure;
b. storing documentations of systems as a preparation for when there is a need to reinstall a system to production server;
c. managing data archive according to retention period;
d. destroying data of which its retention period has ended.

3.4. IT OPERATION RISK MANAGEMENT

The processes of risk management are to identify, to measure, to control, and to monitor risks on functions related to IT operations.

3.4.1. Identification of IT Operational Risk

The process of identification begins with a comprehensive understanding on how Bank operate IT to support organization objectives and then identifying existing risks. The management must consider the events or activities that will possibly disturb operations, amongst others:

a. Errors/mistakes on technology investments including inappropriate implementation, failures on the side of suppliers, incorrect definition of business requirements, conflict with existing systems, or obsolete software (including the loss of vendor support on hardware and software used by the Bank;

b. Problems on system developments and on implementations including insufficiency of project management, cost and time over limit, errors on programming, fail to integrate or migration from an existing system, or mistakes on a system to achieve user requirements;

c. Problems on system capacity such as poor capacity planning, insufficiency of capacity in accommodating system flexibility, insufficiency of software in accommodating business developments;

d. System failures included in network, interface, hardware, software, or failures on internal communication; and

e. Violations on security system including violations on internal and external security, fraud in programming, or viruses in computers.

3.4.2. Measurement of IT Operational Risk

Levels of measured risk depend on related factors, which consist of, amongst others:

a. business importance rating;

b. changes on the content of systems or processes;

c. location of access point (internal or external, including internet, dial-up, or WAN);

d. application sources: purchase packages, in-house developed, or the combination of both;

e. content and system criticality level, or the number of affected business unit;

f. complexity of processing types (batch, real-time, client/server, parallel distributed);

g. volume and value of transactions;

h. classification and sensitivity of processed or used data;

i. effects on data (read, download, upload, update or alter);

j. level of experience and capability of IT Management;

k. sufficiency of the number and capability of staff;

l. variety of platform, application and delivery channel;

m. number of user and customer;

n. changes of regulations;

o. existence of new or developing risks from technologies being developed, or risk of obsolete technology; and

p. existence of audit weakness or weakness found in self-assessment.

3.4.3. Control of IT Operation Risk

On every function of existing IT operation, Banks must mitigate identified and measured risks with control methods determined in the policy and procedure of Bank's IT operations. Having been mitigated, Banks must still monitor controlled risks and residual risks because every disturbance on IT operation will affect operation, strategic, transaction, and reputation risk of the Bank.

3.5. INTERNAL AUDIT

Audit on IT operations is required to ensure proper risk management of IT operation. Detailed regulation concerning internal audit is discussed in Chapter IX regarding IT Internal Audit.

CHAPTER IV
COMMUNICATION NETWORK

4.1. INTRODUCTION

Development of communication network technology has changed a Bank's business approach to become ignorant to time and place limitations. Banks can provide services of various banking products on-line real-time from every office and other delivery channel, such as; Automated Teller Machine (ATM), internet Banking, mobile Banking, and Electronic Data Capture (EDC), of the Bank itself or of service providers.

Communication network includes hardware, software, and transmission media used to transmit information in the form of data, voice, image and video. The carrying-out of communication networks is much influenced by changes, and so is susceptible to disturbances and misuse. Therefore Banks must ensure the integrity of the network is maintained by implementing policies and procedures of network management properly, maximize network performance, design networks resistant to disturbances, and define network services clearly as well as employing necessary security.

4.2. ROLES AND RESPONSIBILITIES OF THE MANAGEMENT

The security of communication network is a responsibility of all parties in the Bank. In carrying it out Banks must own officers/functions that handle the communication network. Said officers/functions must coordinate with the function of IT security organizers. Banks must ensure the availability and capacity of communication network services maintained by Bank's internal or by service providers, for example are equipment spares and adequate services. The management must ensure adequate monitoring in the operation of communication network and in every development or modification of communication network. The management needs to consider how the expected service requirements are suitable with the current business condition and strategies to be developed.

4.3. POLICIES AND PROCEDURES

Banks must possess policies and procedures as guidelines in implementing communication network technologies, to ensure the continuity of operations and security of communication network are maintained. Therefore Banks must determine a baseline/standard used internally for each platform (such as based on protocol or operation system) and implemented on every communication network of the Bank.

Policies and procedures to be determined at least include the following:

a. Performance measurement and network capacity planning (performance and capacity planning);
b. The security of communication network (network access controls, including remote access);

c. change management (setting, configuration and testing);
d. network management, logging and monitoring;
e. the use of internet, intranet, e-mail and wireless (including the mechanism in using communication network);
f. there available a procedure of problem handling;
g. there available facilities for backup & recovery;
h. sufficiency of contract and the availability of SLA suitable with the Bank's requirements and monitored periodically if the communication network is conducted by service providers.

4.3. RISK MANAGEMENT OF COMMUNICATION NETWORK

Banks must identify probabilities, measure possible impacts, and carry out efforts to manage the risk of using communication network. Based on the measurement result of significant risks, Banks must implement adequate control. Banks must also continuously monitor the handling/response of all the significant risk well handled.

4.4.1. Risk Identification

The use of communication network technology presents various advantages and benefits for Banks and customers, although it still needs consideration of potential risks, including but not limited to:

a. loss of data/information;
b. loss of data/information integrity;
c. transmitted data/information incomplete;
d. loss of information confidentiality;
e. communication network unavailable because of disturbances or disaster;
f. loss of/damage on communication network equipments.

4.4.2. Risk Control

In controlling risk in communication network, Banks must consider the following:

a. Communication Network Design

Communication network must be deliberately designed to be efficient but also dynamic to anticipate future development. In this stage, there are some issues in need of consideration, which are:

1) the selection of communication network topology;
2) capacity planning of communication network;
3) the selection of communication network media;
4) hardware backup, alternative routing or alternative provider;
5) physical and logical security:
   a) placement of network equipments at a location secure from nature disturbances and unauthorized access;

b) parameter setting of network equipment system.

6) Availability of audit trail, at least on the parameter changes and access rights of communication network equipment, and also the use of said right.

b. Access Control

Access control in communication network is very important because the communication network is the main entrance to Bank's information system. If inadequately controlled, it could risk information security. In implementing access control, there are several issues to consider, which are:

1) access to network by users is based on business needs and considering the aspect of information security.
2) separate network based on segments, logically or physically, such as the separation between environment of development and production.
3) if physical separation is not possible, Banks must separate communication network logically and monitor the security access in the network.
4) decision to connect to external network must be in accordance with the security requirements and formally approved by the management before its implementation.
5) implementing control that restricts unauthorized or unexpected network traffic.
6) configuration of network equipment must be well configured. Unnecessary functions or services must be deactivated.
7) the use of network security tools, such as firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS).
8) the use of additional network monitoring devices (network management system) by considering its security.
9) periodic testing on network security, for example with penetration testing.

c. Communication network operation and maintenance

The communication network operation and maintenance must be with consideration on the following:

1) The network operating officer must be clearly assigned by the management, possess adequate ability, knowledge and skill, and is given obligations and adequate authorization to perform his/her functions;
2) Banks must possess an incident response plan for disturbances and attacks on network;
3) Banks must possess a backup facility of network hardware/software, including the tested mechanism of restart/recovery. Said backup facility should have different risks from the main equipments, such as using a different service provider;

4) patch and release must be updated (after internal tests) to ensure how the weaknesses have been repaired.

4.4.3. Monitoring Risk

Monitoring risks in communication network includes the following:

a. Existing audit trail must be monitored regularly to be able to detect discrepancies immediately;

b. Network performance is measured periodically based on the level of availability and response time*;*

c. Banks must monitor the capacity used and needed for business development plan, compared to an attached capacity;

d. Banks must monitor and act upon infiltration/attack on communication network;

e. Banks must periodically review the access granting to users to ensure that it is in accordance with its duty and authorization. In addition, it is also required to review network users which have access to external network.

4.5. INTERNAL CONTROL

4.5.1. Internal Audit

Network audit is to be done periodically by an independent party either Internal Auditor or External Auditor. The scope of network audit including but not limited to communication network performance, logical access, physical access, remote access, communication network infrastructure, documentation of communication network. A more detailed regulation regarding audit refers to Chapter X regarding IT Internal Audit**.**

4.5.2. Documentation

To control the network activity management, Banks must possess a complete and latest network documentation, including but not limited to:

a. network policies, procedures, standards, and minimum baselines;

b. network detailed diagram;

c. list and specification of network software and hardware;

d. list of problems and their response;

e. network monitoring report;

f. network capacity planning report;

g. contracts and SLA with the ~~a~~ third party service providers;

h. documentation of network testing;

i. documentation of network implementation;

j. documentation of network changes accompanied by their reason;

k. list of users and their authorization.

CHAPTER V
INFORMATION SECURITY

5.1. INTRODUCTION

Information is a very important asset for Banks, one related to customers, finance, report or other information. Leakage, damage, inaccuracy, unavailability or other disturbances on information can cause both financial and non-financial losses for Banks. Those effects are not only limited to the Bank, but also to customers, other Banks and even to national banking systems. Considering the importance of information, it must be protected or secured by the entire personnel in a Bank. Information security depends on the security of every aspect and related IT components, such as software, hardware, networks, supporting equipments (such as power source, AC) and human resources (including qualification and abilities).

5.2. DUTIES AND OBLIGATIONS

5.2.1. Board of Commissioners

In their duty of directing and evaluating Bank's policies in the management of Information Technology, the Board of Commissioners should coordinate with directors, amongst others requesting Directors to report the distribution of authority and areas of responsibility of IT Operation work units and IT users, efforts to increase control on information security, as well as determining residual risk for the Bank. The aforementioned evaluation also includes evaluation on the effects of information problems on Bank's business process continuity.

5.2.2. IT Steering Committee

IT Steering Committee is responsible for presenting recommendations to the directors which at least regarding the following:

a. Policy of information security as a part of IT Strategic Plan;
b. The effectiveness of the information security policy implementation in Banks;
c. The effectiveness of mitigating risks to increase Bank's information security.

5.2.3 Directors

Directors responsibility on information security include at least the following:

a. Determine policies, systems and procedures of information security;
b. Support every aspects of information security program;
c. Determine distribution of duty and responsibility for decision making related to information security risk management;
d. Determine tolerable risk level of information security;
e. Evaluate the result of the implementation of information security risk mitigation;

f. Communicate to the work units of IT user and IT Operation regarding the importance of information security for the Bank to achieve the purpose of information security in accordance with existing regulations.

5.2.4. Uppermost Official of Information Security

According to the Director's policy and directive, the Uppermost Official of Information Security is responsible for, amongst others:

a. the management of information security function to be in accordance with valid policies and regulations as well as valid best practices;
b. monitoring the information security implementation in every division or work unit;
c. communicating the information security program including employing means to increase awareness on security (security awareness program)
d. determining the criteria and definition of information security risk measurement;
e. carrying out information security risk assessment including assessing the compliance of each and every division in a Bank on information security, and recommending necessary control;
f. ensuring that a third party with authorization to a Bank's confidential information has implemented information security adequately and consistently;
g. assisting the coordination of BCP testing;
h. coordinating information security efforts with the IT internal audit.

5.3. PRINCIPLES, POLICIES AND PROCEDURES OF INFORMATION SECURITY

5.3.1 Principles of Information Security

Information security at least considers the following principles:

a. ensure that the information being managed is secure on its confidentiality, integrity, and availability in effective and efficient means by considering compliance to existing regulations;
b. considers the aspect of human resources, process and technology;
c. carried out based on the result of risk assessment with consideration to Bank's business strategy and existing regulations;
d. implement information security comprehensively and in continuity, by determining the purpose and policy of information security, by implementing information security control, monitoring and evaluating the performance as well as the effectiveness of information security policy, and by carrying out further refining.

Other that the items mentioned above, Banks need to consider the implementation of international standards in the field of information security such as ISO, IEC, COBIT, IT-IL and national standards such as SNI, with consideration to business complexity which includes variety of types of transaction/product/service and office network as well as supporting technology.

5.3.2. Information Security Policy

Bank’s management must have strong commitment on information security policy. Said policy must be periodically communicated to all employee and related external parties. In addition, there must be periodic evaluations and in the event of important changes. Information security policy must include at least:

a. The purpose of information security, which includes assets management, human resources, physical security, logical security, IT operation security, information security incidents response, and information security in system developments;

b. Management commitment on information security in accordance with business strategy and purpose;

c. Guideline structure in determining control through the carrying-out of Bank’s risk management;

d. Principles and standards of information security, including compliance to valid regulations, trainings and improvement of awareness on the importance of information security (security awareness program), business continuity plan and penalties on violation;

e. Roles and responsibilities of involved parties in information security;

f. Documents or other regulations supporting the policies of information security.

5.3.3. Procedures of Information Security

5.3.3.1. Asset Management Procedure

a. Bank’s assets related to information must be identified, its ownership decided and recorded so as to be properly protected;

b. information asset can be in the form of data (hardcopy or softcopy), software, hardware, networks, supporting equipments (for example power source, AC) and human resources (including qualifications and skills);

c. Information need to be classified for adequate security according to its classification. Examples of said classification are “confidential” information (such as customer’s savings data, customer’s personal information), “internal” information (such as regulation on employee’s salary) and public information (such as information about banking products offered to public). These classifications are formed based on the value, sensitivity, law/regulation and level of importance of Banks.

5.3.3.2. Human Resource Management Procedure

a. Bank’s employees, consultants, temporary employees and employees of service providers who have access to information must comprehend their responsibilities on information security;

b. roles and responsibilities of human resources such as Bank’s employees, consultants, temporary employees and employees of service providers who have access to information must be defined and documented in accordance with the policy of information security;

c. in the agreement and contract with Bank's employees, consultants, temporary employees and employees of service providers, must be stated regulations regarding Information Technology security in accordance with Bank's information security policy. For example is the requirement of clause stating that they must safeguard the confidentiality of information obtained, in accordance with the classification of the information;
d. other than the agreement between Banks and service provider companies, all employees of said companies emplaced in the Bank must sign an agreement to safeguard the confidentiality of information (non-disclosure agreement);
e. training and/or socialization about information security is obligatory for Bank's employees, consultants, temporary employees and employees of service providers. This training and/or socialization are given in accordance with the roles and responsibilities of the employees as well as the service providers;
f. Banks must determine penalties for violations on policies of information security;
g. Banks must determine procedures which regulate issues regarding the obligation to return/restore assets and regarding changing/disabling the right of access of Bank's employees, consultants, temporary employees and employees of service providers which are caused by duty reassignment or end of work period or contract.

5.3.3.3. Physical and Environmental Security Procedure

a. important information processing facilities (such as mainframe, server, PC, active network equipment) must be secured physically and environmentally to avoid unauthorized access, damages as well as other disturbances;
b. physical and environmental security on important information processing facilities includes, amongst others, partitions, entry access control (such as the use of access control card, PIN, biometrics), sufficiency of indoor security equipment (such as alarms, fire detectors and extinguishers, thermometers and hygrometers, close-circuit TV) as well as sanitation (from dust, cigarettes, food/drinks, flammables);
c. the capacity and availability of supporting facilities such as AC, power source, fire alarms must be ensured to support the operations of information processing facilities;
d. assets of service providers (such as server, switching tools) must be identified clearly and adequately protected, for example by implementing sufficient security, dual control or separate emplacement from Bank's assets;
e. periodic maintenance and assessment of information processing facilities and supporting facilities in accordance with predetermined procedures.

5.3.3.4. Logical Access Control Procedure (Logical Security)

a. Banks must have formal user administration procedures (written and has been approved by the management) which include registration, change and removal, of internal or external user (such as vendor or service provider);

b. Banks must determine internal control procedures by providing initial password to users with consideration to the following:
   1) initial password must be changed at the time of the first login;
   2) initial password is given in a secure manner, such as through a sealed envelope or double-sided paper;
   3) initial password is unique to every user and is unpredictable;
   4) owner of user-id especially from Bank's employees, temporary employees and employees of service providers must sign statement of responsibility or agreement of the use of user-id and password when receiving the user-id and password;
   5) default password of operation system, application system, database management system, and network equipment must be changed before being implemented and also change the default user ID.

c. Banks must enforce users to:
   1) Keeps password confidential
   2) avoid keeping record of a password on paper and other places without adequate security;
   3) select quality password that at least:
      a) have minimum sufficient length of password and not easily guessed;
      b) easy to remember and consist of at least a combination of 2 character types (letters, numbers or special characters);
      c) not based on user's personal information such as names, phone numbers or date of birth;
      d) not use common words or words easy to guess by software (to avoid brute force attack), such as the word 'pass', 'password', 'adm', or words common in dictionaries;
   4) change the password periodically;
   5) avoid using the same password repeatedly.

d. Banks must deactivate the right of access if inactive for a certain period of time, determine the maximum amount of failed login attempt and deactivate a password after reaching the maximum failed attempt;

e. Banks must periodically review user access right to ensure it is in accordance with the given authorization.

f. Bank's operation systems, application systems, database, utilities and other equipments should help ensure the securing of password, for example:

1) enforce users to change their password after a certain period of time and avoid historical password;
2) store password securely (encrypted);
3) cut off the connection or user's access when there are no response after a certain period of time (session time-out);
4) deactivate or delete a user's access right if inactive loggin for a certain period of time (expiration interval), i.e annual leave, relocation.

g. Banks must estimate the risks and implement adequate control in the use of mobile computing equipments and data storage media such as notebook, hand phone, personal digital assistance, flash disk, external hard disk, including the case of using wireless access or wireless network;

h. Banks must estimate the risks and implement adequate control on network access points and/or information processing facility that can be used by unauthorized parties;

i. limit access for file sharing, at least enforce the use of password and user access management;

j. Consider the security hardening on hardware and software, such as : setting parameter, patch.

5.3.3.5. Information Technology Operation Security Procedure

Items to consider in IT operation security are, amongst others:

a. Information and software must have a backup and recovery procedure and tested according to its level of importance;

b. anticipate and implement adequate security control on operation system, application system, database and networks, including threats from unauthorized parties such as virus, Trojan horse, worms, spy ware, Denial-Of-Service (DOS), war driving, spoofing and logic bomb;

c. formalize policies and procedures of anti-virus and patch updates, and ensure their implementation;

d. develop a procedure which includes identification of existing patches, testing, and install it if necessary;

e. maintain a record of current software version and routinely monitor the information regarding updates (enhancement) of products, security problems, patches or upgrades, or other problems in accordance with the current software version;

f. implement the use of encryption by using a particular cryptography technique in securing the process of sensitive information transmission, especially connection to external network, in accordance with the development of the latest technology. The uses of cryptography technique are, amongst others, aimed to safeguard and ensure confidentiality, integrity, authenticity, and non-repudiation. Considerable techniques are, amongst others, the use of encryption, hash function, and digital signatures (using Public Key Infrastructure)*;*

g. implement identification and authentication method in accordance with the level of importance of applications, such as one-factor authentication for “common” application as well as the use of two-factor authentication for “critical” application;

h. Examples of identification and authentication method are, amongst others, log on id and password, token device or biometrics (such as fingerprint, retina scan, face/iris/hand/palm analysis, signature recognition, voice recognition);

i. review audit trail/log in network, system or application level, as well as determine the type of the log (such as administrator log, user log, system log), information required in the log, storage duration or log capacity with consideration on valid regulation for problem trailing.

5.3.3.6. Information Security Incidents Response Procedure

Items to consider in handling information security incidents are, amongst others:

a. incidents must be identified, reported, acted upon, documented and evaluated to ensure proper handling and to avoid reoccurrence;

b. Banks must determine procedures of incidents response which regulate:
   1) Who to report incidents;
   2) The type of incidents to be reported;
   3) Flow of incident reporting (point of contact);
   4) Who is responsible to act upon incidents;
   5) Analysis on incidents to avoid reoccurrence;
   6) Documentation of incident-related evidence and follow ups.

c. Banks need to consider the forming of special teams to handle security incidents (CSIRT – Computer Security Incident Response Team or CERT – Computer Emergency Response Team) in accordance with the scale of business and Bank’s IT complexity;

d. Bank’s employees, temporary employees, and service provider employees are required to report on every indication or potential of weakness on the system and application in accordance with the policy and procedure of security incident report. An example of weakness to report is a virus from an e-mail.

5.3.3.7. Other Procedure

Other than the scope mentioned above, information security must be implemented in other aspects such as system development and establishment, data communication network, BCP and DRP and the activity of using IT service providers.

5.4 RISK MANAGEMENT PROCESS

5.4.1. Risk Assessment

Considering the importance of IT in supporting the achievement of Bank's business strategic plan, Banks must manage every IT resource as an asset of the Bank. IT resources include, amongst others, applications, information, infrastructure and human resources. Therefore, Banks must perform evaluation on all that threaten IT resources through the process of identification, measurement and monitoring of potential risks in their tendency or probability of occurrence or the magnitude of the effect.

There are several approaches of identification such as approach by process, assets, products, and occurrences. In the approach based on assets, the identification of security risks are conducted through a classification on "assets" related to information technology based on risks. Afterward, Banks measure the tendency or probability of risk occurrence on every asset and the magnitude of losses caused, to recognize potential risks or Base Risk Value (NRD). Examples of information security risk assessment using the method of assets are available in Index 1.1. This assessment is done by every work unit possessing IT resources and/or can be coordinated by work unit of IT or risk management field. In determining critical assets or measuring risks, each and every work unit must be able to determine the probability of threats, attacks and vulnerability from every IT resource used by each work unit as well as possible effects on integrity, confidentiality and availability of existing data/information. This process must be carried out because identification and measurement of risks can show the potential of failure or weakness of information security process which can influence the success of Bank's business so Banks are able to act proper response on every potential risk.

5.4.2. Risk Management and Mitigation

Based on the result of risks identification and measurement, Banks must determine type of risk handling to be implemented. From type of risks response (accept, control/mitigate, avoid, transfer), risks control and/or mitigation holds an important role because without reliable information system and effective IT control activities, Banks will not be able to present accurate, latest, total and complete reports. In general, types of control are, amongst others:

a. policies, regulations and procedures in a Bank;
b. risks control system using technologies so to automatically mitigate existing risks such as audit log, on line approval, parameter value in the system used;
c. training and security awareness program.

Controls monitoring are done twice where the first time is on the process of risk assessment where Banks identify previous controls, and the second is after receiving

Final Risk Value (residual risk). By comparing Base Risk Value (NRD) with Final Risk Value (NRA), Banks can analyze the weaknesses of the previously implemented controls and recommend a new type of security control to be implemented afterwards. Type of controls can vary and not be limited to general controls such as controls that must be present in Data Center operations, or one in the form of application controls such as reconciliation in balancing control activities. And so every Bank's asset in the level of Bank, work unit or individual official/user can avoid potential risks.

5.5. INTERNAL CONTROL AND AUDIT

IT Internal Auditor must carry out audit programs to ensure that information security control has been implemented, is adequate and running effectively in accordance with valid policies and procedures of information security. Internal control must be implemented in information security because information security is a dynamic process that must be carried out in continuity. Evaluation and completion on policies, procedures and programs of information security must always be conducted, amongst others by carrying out monitoring on:

a. development of new techniques or methods that threaten Bank's information security system;
b. reports of information security performance to identify trend of threats or weaknesses to security control. More specifically this activity includes review on activities log, operation anomaly investigation and routinely evaluate access levels on IT systems and applications;
c. ensuing actions in the response on attacks or incidents in information security;
d. the effectiveness of the implementation of information security policies, procedures and controls;
e. potential risks prevention activities on the probability of threats on information security/information system such as:
    1) processes which monitor the threats to hardware/software, security patches installation;
    2) review of anti virus update;
    3) monitoring third parties/vendor service.

Monitoring on information security includes technical and non-technical aspects. Non-technical aspect includes organization changes, business process changes, new location, sensitivity level changes or new products/services publishing. Technical aspect includes new system, new service provider, and expansion/addition of access to information. Monitoring can be done by information security officer or in case the Bank do not have one then by an employee functioning in managing information security program. However, every employee and management must be aware of threats to information security/information system.

CHAPTER VI
BUSINESS CONTINUITY PLAN

6.1. INTRODUCTION

Banking activity can not be avoided from disturbances/damages by nature or by human, for examples earthquake, bombs, fire, flood, power failure, technical problems, human errors, worker demonstration, riots and the like. Those damages do not only affect a Bank's technological capabilities, but also affect the Bank's business operations especially services to customers. If not handled properly, other than facing operational risks, Banks would also suffer reputation risks and could impact to the decline/decrease of customer's level of trust to the Bank.

To minimize those risks, Banks are expected to have Business Continuity Management (BCM) which is an integrated management process to guarantee that Bank's operations are functional in the event of disturbances/disaster for the purpose of protecting the interest of stakeholders. BCM is an integrated part of the Banking's risk management policy. An effective BCM needs to be supported with the following:

a. active management monitoring;
b. Business Impact Analysis and Risk Assessment*;*
c. adequate Business Continuity Plan*;*
d. testing on BCP; and
e. reviewed by Internal Auditor.

Business Continuity Plan (BCP) is a written document which contains an arrangement of planned and coordinated activities regarding steps to decrease risks, responses on disturbance/disaster effects and recovery process for the continuity of Bank's operations. The written plan of action involves every IT resource including human resources which support business functions and critical operational activities to the Bank.

Components of BCP procedure in a Bank at least include Disaster Recovery Plan (DRP) and Contingency Plan (CP). Disaster Recovery Plan (DRP) stress more on technological aspect with focus on data recovery/restoration plan and the functioning of critical application systems as well as IT infrastructure. On the other hand Contingency Plan *(CP)* emphasize more on action plan to maintain business continuity in the event of occurring disturbances or disaster, including anticipation actions for the worst scenario such as when the IT being used can not be recovered in any way for quite a long time. Contingency Plan (CP) must also include plans of ensuring the continuity of all the Bank's services including services through electronic banking.

6.2. ACTIVE MANAGEMENT MONITORING

The effectiveness of BCP will very much depend on the management commitment to provide necessary resources in the event of identifying, arranging and testing in BCP.

6.2.1. Roles and Responsibilities of Directors

a. determining policies, strategies, and procedures of BCP;
b. determining BCP which is to be updated periodically;
c. ensuring the existence of an organization or a work unit responsible over the BCP, which includes competent and trained personnel;
d. ensuring the BCP to be socialized to every function of business and personnel;
e. review the result of BCP regular tasting;
f. evaluating the result of internal audit on the sufficiency of BCP.

6.2.2. Roles and Responsibilities of BCP Work Team

For the BCP to run properly when necessary, banks need to form an organization or a work team to coordinate the carrying-out of BCP, which consist of:

a. coordinator;
b. team members with responsibility on:
    1) business units;
    2) IT units, amongst others, offsite storage, applications, hardware and software, networks, security, communication, data preparation and records*;*
    3) other supporting units such as Logistic, Security and General, Public Relation and Legal, Human Resources.

The role of work unit in charge of BCP mentioned above at least includes:

a. fully responsible on the effectiveness of BCP, including ensuring that the awareness program on BCP is implemented;
b. determine condition of disaster and its recovery;
c. determine recovery scenario to be used in the event of disturbances or disasters, based on priority of activities, functions and services deemed critical;
d. review reports regarding every stage of testing and conducting of BCP;
e. communication to Bank’s internal and external parties in the event of major operational disturbances.

6.3. PRINCIPLES OF BCP ARRANGEMENT

In arranging policies, strategies and procedures to be implemented for response on disaster, Banks must ensure the implementation of the following principles:

a. arrangement of BCP should involve all business units and functions, not only IT;
b. BCP is arranged based on adequate Business Impact Analysis and Risk Assessment;

c. BCP is formed flexible to enable response to various threat and disturbance scenarios of unpredictable nature, that come from internal or external condition;
d. BCP is formed to be specific, to have certain conditions and immediate necessary actions for such conditions;
e. testing and updates are done periodically;
f. BCP and the result of BCP testing must be reviewed by internal audit periodically.

6.4. BUSINESS IMPACT ANALYSIS

Effectiveness of a BCP will very much depend on the ability of the management to accurately identify whether various work processes or activities in a bank before the BCP is arranged or reviewed, is critical or not. As it is, Business Impact Analysis (BIA) is the base of the arrangement of the entire BCP. Items to analyze in BIA include:

a. levels of importance (criticality) of each business process and dependence between business process as well as necessary priorities;
b. levels of dependence on IT or non-IT service providers;
c. the level of Maximum Tolerable Outage/Recovery Time Objective (how long the bank can operate without the systems or facilities experiencing a disturbance and/or how fast systems or facilities must function back on);
d. the level of Minimum Resources Requirement (minimum personnel, data and sufficiency of systems as well as facilities for business to recover and operating);
e. potential effects from unspecific and uncontrollable occurrences on the process of business and service to customers;
f. impacts of disaster on every department and functions of business, not only on data processing;
g. estimation of maximum tolerable downtime and levels of tolerance on the loss of data and a halt in business process as well as the impact of downtime on financial loss;
h. necessary communication line for recovery;
i. capability and knowledge of officers/officials regarding Contingency Plan and the availability of replacement officers at the place of recovery;
j. legal impacts and the fulfillment of related regulations, such as regulation regarding customer’s information confidentiality.

In carrying out the above mentioned BIA, IT units or each business unit need to consider how the arranged BCP is not only for the event of total disaster, but for various situation of disaster and disturbance, beginning from a minor, major, to a catastrophic one.

And so the impacts need to consider are not only the one that can be clearly measured (tangible impact) such as penalties for delays on interest payment or employee's overtime cost, but also for one that can not be clearly measured (intangible impact) such as the difficulty for customers to get services.

6.5. RISK ASSESSMENT

Risk assessment which consists of identification and measurement of risks is the second stage in the arrangement of a BCP. This process is necessary to recognize the probability of disturbances on important (critical) bank activities as well as its impacts to the continuity of bank's business. Risk assessment at least includes the following:

a. Performing analysis on the impacts of disturbances or disasters on banks, customers and financial industries;
b. Performing gap analysis by comparing the current condition with steps or scenarios which are supposed to be implemented;
c. create ratings of business disturbance potential based on its severity and likelihood.

6.6. BUSINESS CONTINUITY PLAN ARRANGEMENT PROCESS

The arrangement of BCP is after the process of BIA and Risk Assessment. The purposes and aims of BCP arrangement are, amongst others:

a. securing the bank's important assets;
b. minimizing risks from disaster such as through limiting financial losses, legal risks and reputation risks;
c. ensuring the availability of services in continuity for customers; and
d. preparing other alternatives so that critical business functions can still operate to maintain the continuity of bank's operations.

BCP consist of policies, strategies, scenarios and procedures necessary in ensuring the continuity of business processes in the event of disturbance or disaster. BCP must include several possible alternative strategies to handle each and every type of disturbance or disaster and their magnitude. The recovery strategies are adjusted to the result of BIA, risk analysis, resources, as well as the capacity and level of Bank's technology. Examples of possible strategies are, amongst others, the use of other parties (outsourcing), Disaster Recovery Center (hot site, warm site or cold site) and/or Business Recovery Center. Every chosen strategy should be accompanied by the background analysis/reason and must be supported by suitable systems and procedures.

6.6.1.Types of BCP Procedures

Types of procedure in BCP should at least include:

a. emergency response procedure (immediate steps) to control the crisis in the event of disturbance/disaster, to limit losses, as well as to determine the need to declare a condition of disaster*;*

b. system recovery procedure which enables Bank's operations to return to normal condition;

c. business recovery procedures which defines the duty and responsibility in each business process to recover Bank's operations. Included here is the contingency plan for manual customer service when necessary;

d. data synchronization procedures is used to ensure that the data from production machines are the same with the data on backup site, as well as to ensure all data as the result of business processes during recovery period have been placed in the system.

6.6.2. Components of BCP Procedures

Every BCP procedure mentioned above should include at least the following components:

a. Personnel:

When necessary, sub teams can be formed in the organization of BCP work team for coordination, conducting of emergency response procedure, conducting of system recovery, conducting of business process recovery and evaluation or feedbacks. BCP must clearly state the composition, authorization and responsibilities of every BCP work team, and possess integrated communication lines.

b. Technology:

Procedures must consider components of technology of a Bank such as hardware, software, communication facilities, include equipments of operation processing activities in each business function.

Other than items related to data files and vital records, also in need of other consideration such as the existence of DRC and system documentation and backup data.

c. Disaster Recovery Center (DRC):

Banks must ensure the availability of DRC as DC backup which is able to operate if the DC is down or in the condition of disaster. In accordance with the chosen alternative strategy, DRC can be managed by the Bank itself of by service providers. Banks must consider the following:

1) DRC should be placed in a separate location from DC, with consideration on geography factor:

   a) geographical reach of a disturbance/disaster and its impacts on the city or area where DRC is located;

   b) risk analysis related to the location of DRC (of earthquake or thunder areas) and connected to different communication and power infrastructure from DC, as well as other facilities necessary to maintain a system;

2) hazard level of selected location with regards to the possibility of riots and civil unrest;
3) DRC must have a power supply and telecommunication facility that guarantee the DRC being operational;
4) systems in DRC must be compatible with the system used in DC and must be adjusted if there are changes on DC;
5) is a restricted area; and
6) estimates the travel duration to guarantee the process of recovery.

d. Documentation, System and Data Backup

Banks must ensure the availability of effective backup of important business information, software and documentation related to system and user for each critical business function process. Items need to be considered in documentation, system and data backup are, amongst others:

1) backup must be stored in a different location from DC (off site). Every changes and modification must be documented and their copies must also be updated;
2) backup media must be stored in a secure environment in off site location with adequate security system standard;
3) full system backup must be done periodically. In the event of fundamental system changes then full system backup must be done immediately;
4) every backup media use labeling/naming standard to be able to identify the use, date and schedule of retention;
5) backup media must be tested regularly to ensure that said backup is available when it is necessary (emergency situation);
6) Banks must possess procedures for backup media disposal.

e. Business Recovery Center (BRC)/Crisis Center/Business Resumption Center

BCP must possess scenarios concerning the location of activity of each business function for various levels of disaster. For levels of total disaster or catastrophic, Banks should prepare an alternative location to remain capable of carrying out business function activities.

f. Communication Facilities

Banks must ensure that alternative communication lines in Bank's operational regions are available in the event of disturbance/disaster, in internal environment or external.

6.7. BCP Testing

The testing of BCP is needed to ensure that BCP can operate well in the event of disturbance/disaster. Tests on BCP and DRP conducted at least once every 1 (one) year for all critical system/application (in accordance with the result of Business Impact Analysis) and represent every critical infrastructure as well as involve end users (end to end).

If a Bank uses the service of a service provider in its operations then the tests are required to involve the external party. In the case where a Bank carries out a very fundamental change on the system, application or infrastructure of its information technology (such as changes on the core banking system), then tests on DRP must be done 6 months after the implementation of the system changes at the latest.

6.7.1. Scope of BCP Testing

The management must clearly determine the functions, systems and processes to be tested. Items that required testing include the effectiveness of:

a. personnel evacuation route and determined communication line (*call tree*);
b. disaster condition declaration procedure;
c. facilities of DRC and BRC provided by other parties for only one Bank or used mutually with other Banks;
d. recovery procedure on important data;
e. the return of Bank's operations and Data Center to the initial location of business unit and data center.

Tests must be documented orderly and evaluated to ensure the effectiveness and success of the tests. If in the testing are discovered weaknesses on BCP, then BCP needs to be improved.

6.7.2. Test Plan

Banks must possess test plans for every test that are going to be carried out and the plans sufficiency must be studied. The carrying-out of said plans must not disturb Bank's operations. The results of the tests are expected could detect weaknesses on existing procedures in BCP recovery.

In this case Banks must validate the assumption used in the test plan, regarding, amongst others:

a. the significance of business function processes or tested system;
b. transaction volume;
c. dependency between business processes;
d. selected BCP strategy;
e. the availability and sufficiency of necessary resources to be suitable to the determined service level, such as necessary time to prepare existing facilities, backup file or to prepare documents.

6.6.3. Analysis and Report of Test Result

The result of test and analysis of each discovered problems during the test must be reported to the directors. Items to be reported at least include:

a. assessment of test purposes achievement;
b. assessment on the validity of data processing test;

c. correction actions to solve occurring problems;
d. description about discrepancies between BCP and the test result as well as the suggestion of its changing;
e. recommendation for subsequent tests.

In the event of failures on test results then Banks must review the cause of the failure or the occurring problems and repeat the test.

6.7. MAINTENANCE OF BCP AND INTERNAL AUDIT

6.7.1. BCP Maintenance

Banks must ensure that BCP is available at all time, amongst others by storing copies of BCP documents in an alternate site, by increasing the understanding of all concerned parties in a Bank or service provider on the importance of BCP and be actively participate in the carrying-out of BCP. Every core/main personnel in BCP work team must possess a summary of BCP emergency response procedure as well as the most recent contact person list to notify in the event of disturbance/disaster (*call tree*).

Beside that every work unit must periodically carry out self assessment of Business Impact Analysis accordance with changes in operations by the Bank itself or by service providers.

Banks must update the BCP to ensure its compatibility with external or internal condition. In updating, items to be considered are, amongst others, changes on business processes, organization structure, systems, software, operating system, hardware, personnel/key staff, facilities, counterparties and service. The changes must be analyzed of their impacts on the currently existing BCP and Banks must decide necessary restoration to accommodate the changes in the new BCP. Then the revised BCP must be documented and distributed to the entire organization*.*

6.7.2. Internal Audit

Internal Auditor must perform assessment on:

a. accordance of BCP with the Bank's risk management policy;
b. BCP includes critical activities based on Business Impact Analysis;
c. sufficiency of BCP to control and mitigate risks determined in risk assessment;
d. sufficiency of BCP testing procedure;
e. the effectiveness of BCP tests;
f. BCP training and socialization program;
g. latest version BCP in accordance with the development of Bank's operations and final test result.

Internal Auditor must communicate the result of the assessment and suggest recommendations to the directors. Directors should review the report of said audit result.

CHAPTER VII
END USER COMPUTING

7.1. INTRODUCTION

End User Computing (EUC) is a computer application system which carries out Bank's business operations where control on the development of application system as well as its management are carried out by end user or Bank's business units, and not by IT.

Some reasons of the use of EUC in a Bank are, amongst others:

a. the existence of delayed development project of application systems (backlog project) by IT, causing EUC to enable end users to develop, maintain, and operate IT by themselves;
b. the existence of specific requirements from users, with few users and little volume, therefore it would be less efficient when going through the procedure of application system development in general by IT .

7.2. ROLES AND RESPONSIBILITES OF THE MANAGEMENT

In its relation with EUC, the Bank's management must ensure that:

a. possible risks related to EUC are managed adequately;
b. EUC can increase the users performance. EUC application system can be used to fill the requirements in analyzing data, making reports, and carrying out query which enables the process of decision making to run more effectively and efficiently;
c. EUC can only be used to fill the requirements of simple application system, can fill requirements that always change, or to give fast response on urgent or temporary requirements;
d. EUC can decrease the delay of making an application system (backlog);
e. Delay on the fulfillment of new application system modification or development requirements will decrease because EUC lessen the burden of information technology system development by IT.

7.3. EUC POLICIES AND PROCEDURES

Items to be regulated in Bank's policy and procedure regarding EUC include, amongst others:

a. policies and procedures must be written, approved by Directors/authorized officials, reviewed and updated periodically, as well as socialized to all end user;
b. clear definition of authorization and responsibilities of the management, related business working unit, IT working unit, as well as internal audit;
c. analysis on EUC application system development requirements and its approval procedure;

d. development of EUC application system must fulfill the standard and criteria of security determined by IT working unit;

e. application system enabled to be developed in the way of EUC is the application system with “low” to “moderate” level of complexity and risk and must be through the approval of the management;

f. stages of EUC application system development, from the establishment to the implementation;

g. change procedure on EUC application system;

h. fulfill the aspects of security (physical and logical), EUC application system control (control on input, process, and output), operational control including virus prevention;

i. availability of the most updated list of existing EUC application system;

j. storing and backup of data/files;

k. availability of adequate documentation, including, amongst others, user manual and system manual. Every change on EUC application system must be accompanied by the updating of the documentation;

l. if the application system is made by vendor, end users must coordinate with IT working unit. Beside that the management must ensure the sufficiency of training and manual arranged as a part of the contract between Bank and vendor;

m. if the application which is developed by vendor caused the Bank to be dependent to the service of the developer, then the selection of vendor is conducted through a process which refers to guidelines regarding Information Technology Service Provider Usage as well as Bank’s internal policies and procedures;

n. EUC development policies and procedures can not contradict existing policies especially the system development (SLDC) policy as well as the information security policy.

7.4. EUC RISK MANAGEMENT

7.4.1. Identification and Measurement of EUC Application System Risks

Banks must define levels of risk for every EUC application system periodically. If an application system possesses high level of risk then the developments including their maintenance must be carried out by IT.

Several risks related to EUC are, amongst others:

a. if EUC does not fulfill adequate security standard, then there are possible risks of unauthorized access which can cause data/information leakage as well as fraud which further cause financial or non-financial loss;

b. inadequate documentation of application system can cause dependency on personnel who develop and are familiar with the system (key person);

c. application system being developed is inadequate, is caused by, amongst others:

1) lack of understanding on possible risks might be happen in the future;

2) lack of competence and end users experience in application system development;
3) the use of technologies without consideration on Bank’s condition and business requirements.

d. development and the use of a system by each end user can cause confusion regarding responsibilities on system ownership, data as well as response on occurring problems;
e. declining integrity and accuracy of Bank’s data/information;
f. absence of adequate audit trail so as to cause limitation on Bank’s capability of trailing, such as in case of fraud presumption.

By observing the risks mentioned above, EUC must be conducted through coordination between user and IT. Users can develop their own application systems, but IT must manage the inventory of the application systems, and evaluate their accordance with Bank’s development policies and procedures. If similar applications are needed by another working unit then EUC can be implemented to the working unit with the same necessities. There are several methods of risk measurement for Banks. If a Bank use a Control Self Assessment (CSA) in assessing risks, then the Bank must include EUC to the scope of CSA done by each working unit. Every Bank by itself can determine risk appetite adjusted to the scale and condition of the Bank involved. Examples of categorization of levels of risk are available in index 1.2.

7.4.2. Risk Management and Risk Mitigation

Considering possible risks in EUC application system, the development and the use of EUC application system should only be conducted if the user requirement is urgent, detail, various, and/or if the use of said application system is temporary. Beside that Banks must always perform adequate control on EUC. Forms of control that must be implemented include at least the following:

a. Control on developments, testing and changes of EUC applications are, amongst others:
   1) every EUC application to be developed must be reported to IT;
   2) IT must provide approval/certification before the application is made available by user. Approval is given after an analysis of application sufficiency from functional aspect, security (physical and logical), as well as the accordance of application with the user requirements;
   3) IT must take inventory of all EUC application used by user working unit, including every existing addition and modification;
   4) in the event of addition or modification on the application, user must report and obtain approval from IT as mentioned in letter a and b;

5) to keep and protect the confidentiality of program and data from unauthorized parties, Banks must possess security actions on data, source code and executable files.

Beside that, Banks must also consider general principles of application development control as regulated in Chapter II Development & Acquisition.

b. Security standard on every EUC application by referring to Information Security Policy as mentioned in Chapter V. Necessary Information Security to minimize operational risks. The standard includes at least the following:

1) Validation process is necessary for data input into EUC application manually or inter-computer transmission (download, upload or electronic transfer) through a network to guarantee data integrity;
2) Adequate control on data preparation stage, input, processing, output distribution, and reconciliation process to be implemented by the Bank. Such are implemented especially on EUC application used to process Bank's or customer's financial information, for the purpose of guaranteeing data integrity and availability of audit trail;
3) Bank's management needs to backup EUC data and application periodically. Beside that, Bank's DRP and BCP must estimate the risks related to EUC application.

7.5. INTERNAL AUDIT

Items to consider related to audit on EUC application are, amongst others:

a. EUC application is included as assessment objects of IT internal audit working unit;
b. audit is done periodically to ensure that the implemented control are adequate and effective;
c. Banks must ensure there are ensuing actions on findings from audit result.

CHAPTER VIII
ELECTRONIC BANKING

8.1. INTRODUCTION

Information Technology and globalization significantly advance support the Bank to increase services to customers securely, comfortably and effectively, amongst others through electronic media or better known as e-banking. Through e-banking, Bank's customers in general can access banking products and services by using various electronic devices (intelligent electronic device) such as personal computer (PC), personal digital assistance (PDA), automatic teller machine (ATM), kiosk, or telephone.

In this guideline Electronic Banking (e-banking) is define as the service enables Bank's customers to obtain information, communicate, and having banking transactions through electronic media such as Automatic Teller Machine (ATM), phone banking, electronic fund transfer (EFT), Electronic Data Capture (EDC)/Point Of Sales (POS), internet banking and mobile banking. In offering e-banking services, Banks can provide services of informational, communicative and/or transactional nature. In providing e-banking services Banks should consider the principle of prudential banking, the principle security and integrity of IT system, cost effectiveness, adequate customer protection as well as being in the same direction with Bank's business strategy.

Considering that e-banking is an alternative delivery channel, aside from facing existing risks, there are also additions and increases of operational risks, legal risks and reputation risks which originate from the use of Information Technology.

8.2. ROLES AND RESPONSIBILITIES OF THE MANAGEMENT

The Commissioners and Directors must perform effective oversight on risks related to e-banking activities, including setting out of accountability, policies, and processes of control to manage such risks.

8.2.1. Board of Commissioners

a. Commissioners must put in place policy guidelines related to plans of e-banking activities and evaluate the accordance of such plans with the Bank's Information Technology strategic plan and business strategic plan;
b. Commissioners must oversee on the carrying-out of policies related to e-banking activities.

8.2.2. Directors

a. Directors must review the implementation of e-banking plan with the potential of significant impacts on Bank’s strategy and risk profile including cost and benefit analysis of such plan;

b. Directors must ensure that when a Bank begins the e-banking activities, it already has adequate risk management. In addition, Directors must ensure that the officials or employees related to the activities of e-banking are competent in the applications and technologies supporting e-banking;

c. Directors must monitor periodically on the risks attached to e-banking, and report the result of said monitorto the Commissioners;

d. Directors must ensure that the process of Risk Management of e-banking activities is integrated in the Bank’s Risk Management as a total. Policies and procedures of risk management must be evaluated to anticipate additional risks which originate from the activities of e-banking. And so Banks must perform the following steps:

    1) determine the limit of risk in its relation with e-banking with consideration to the Bank’s risk appetite;

    2) determine an authorization delegate and report mechanism, including necessary procedures for occurrences that affect Bank’s financial condition and reputation;

    3) consider risk factors which especially relate to security, integrity and availability of e-banking services;

    4) ensure that adequate complete testing (due diligence) and risk analysis has been done before Banks perform transactional e-banking activities by cross border.

e. when the system of e-banking is conducted by other parties (outsourcing), Banks must determine and implement procedure of monitoring and due diligence as a total and continuously to manage the relation of Banks and those other parties;

f. in reviewing the main aspects of Bank security control procedure, directors must:

    1) continuously supervise development and maintenance on the infrastructure protecting the Bank’s e-banking systems and data from internal and external disruptions;

    2) ensure that the Bank possess policies and procedures of entire security control to handle security threat potentials both from internal and external, in the form of preventive actions or incidents response. The mentioned procedure of security control should includes:

        a) assignment of responsible Bank’s officials to observe the arrangement and maintenance of Bank security policy (corporate level security policy);

        b) adequate physical control to prevent unauthorized physical access to computer rooms;

c) logical control procedure and adequate monitoring and testing of user in order to prevent internal and external unauthorized access into applications and database of e-banking transactions;

d) periodic reviews and tests on system security steps for e-banking.

3) ensure the implementation of risk management by IT unit and e-banking operational work units. Among others are self assessment in the form of measuring and monitoring related e-banking risks, and the usage of self assessment result to determine the Bank's policies and procedures for e-banking security.

8.3. POLICIES & PROCEDURES

To manage risks within e-banking products and activities, Banks must have written policies and procedures for each product, which at least cover the followings:

a. standard operating procedures of e-banking products and activities;
b. responsibilities and authorization in managing e-banking products and activities;
c. accounting information system of e-banking products, including it's correlation with Bank's entire accounting information system;
d. procedures in identifying, measuring and monitoring risks within e-banking products.

Each product's standard operating procedure must satisfy the security control principle of customer's information and e-banking transaction, which are:

a. confidentiality;
b. integrity;
c. availability;
d. authentication;
e. non repudiation;
f. segregation of duties;
g. authorization of control on system, database and applications;
h. maintenance of audit trails.

In determining security control of e-banking activities and products, Banks should also consider other parties related to e-banking services, apart from considering the service's security to customers.

8.4. RISK MANAGEMENT OF E-BANKING ACTIVITIES AND PRODUCTS

8.4.1. Risk Assessment related to E-Banking

Banks must identify risks that may arise from e-banking activities, whether resulting from the product itself or from use of Information Technology as consequence of using electronic delivery channel.

Calculation shall be done on each loss event of every products. To be able to monitor the scale and probability of risk from each products, Banks must develop a database of historical data on losses from every products (loss event database).

8.4.1.1. General Risk

General risks comprise:

a. Transaction/Operations Risk: risk arising or resulting from fraud, errors in process, system disturbance or unpredictable activities which cause Bank's inability in providing products or services, and at the same time causing losses to Bank or customers. Transaction risk includes risks arise from unsatisfactory implementation of security control principles mentioned above;

b. Credit Risk: credit risk may arise when Bank provides credit facility using electronic media, such as credit card;

c. Compliance/Legal Risk arises from:
   1) noncompliance to law and/or regulations set by supervision authorities;
   2) disparity with other countries' law in term of cross border transaction;
   3) noncompliance to regulations on customer's information confidentiality and product information transparency;
   4) limitation on regulations, serving as the legal basis of e-banking transactions.

d. Strategic Risk, may arise from;
   1) Inconsistency to Bank's business purposes/plans;
   2) unwell-prepared e-banking investment plan may cause lesser return on investment compared to expenditure;
   3) unwell management of relation with IT service providers (relationship management);

e. Reputation Risk: reputation risks arise from the possibility of decrease in or loss of customer's trust because the service level delivery to customers is not well-maintained, for example unprompted or unavailable e-banking service, slow response to customer's complaints, unsecured system and disturbances on the system.

f. Market Risk: risks that arise when Bank provides a product with features enabling execution of transactions exposed to interest rate change, exchange rate fluctuation, for example internet banking transfer service from IDR account to a foreign currency account located overseas.

g. Liquidity Risk: risks that arise when Bank does not limit the amount that may be transferred by corporate customers via internet banking.

8.4.1.2. Specific Risk

In conducting e-banking activities, Bank will face specific risks as a result of providing and using Information Technology. These risks will increase Banks' risk exposure. Examples of specific risks are, amongst others:

a. Operational risks that may arise from e-banking transactions are fraud, skimming, errors, damages or non-functioning systems;

b. Risks that may arise from cross border e-banking transactions, one of which is legal risk due to the transactions crossing different legal territories. This risk arise due to disparity between regulations of two legal territories, such as consumer protection regulation, Bank secrecy and customer's personal information confidentiality, reporting requirement and money laundering regulation. Apart from that, Bank may also face other risks such as operational risks, credit risks and market risks;

c. Risks in operating internet banking comprise:

   1) customers obtaining incorrect or inaccurate information through the internet;
   2) financial data theft from Bank's database via unisolated informational and communicative internet banking;
   3) threats/attacks, for examples: defacing, cybersquating, denial of service, network interception, man-in-the-middle-attack, viruses.
   4) identity theft, for examples: phising, key logger, spoofing, cybersquating;
   5) unauthorized transactions or fraud.

d. Security threats on products using wireless technology such as mobile banking are, amongst others, communication intrusion or interception due to unencrypted mobile banking transaction, denial of service attack, virus, worm, Trojan, replication of sim card and hand phone number;

e. Security threats to phone banking products which are very susceptible to interception.

8.4.2. Risk Mitigation

Bank must perform mitigation on general risks and specific risks that may arise in e-banking service, with due observance to customer's data and e-banking transaction security control principle.

8.4.2.1. Principles of Security Control On E-Banking Activities

a. Bank must perform satisfactory steps to test the identity authentication and authorization of customer conducting e-banking transactions, with due observance to the followings:

   1) Bank must have written policies and procedures which ensure that Bank is capable of testing customer's identity authentication and authorization.

2) Bank may use various methods to test authenticity based on risk management assessment of e-banking activities, sensitivity and value of stored data. In effecting authenticity test method, Bank should observe the followings:
   a) Implement combination of at least two factor authentication, i.e. “what you know” (PIN, password), “what you have” (magnetic cards with chips, token, digital signature), “something you are” or “biometric” (retina, fingerprint);
   b) PIN minimum characters requirement. Particularly for PIN on card-based payment instrument, mobile banking and internet banking, PIN should consist of at least 6 characters;
   c) Employ maximum attempt of incorrect PIN input, in order to avoid unauthorized access;
   d) Banks must ensure the implementation of prudential principle in employing authenticity test method, which include:
      (1) creation, validation and encryption of PIN and other methods of authenticity test must use secured methods;
      (2) database of authenticity test which provides access to customer’s account in e-banking, protected from disturbance and damage;
      (3) each addition, deletion or alteration on database of authenticity test has been properly approved by authorized parties;
      (4) particularly for card-based e-banking services, the function of creating and delivering PIN must be separated from the function of creating and delivering card;
      (5) appropriate control facilities of e-banking systems must be put in place, so any unregistered third party can not replace a registered customer;
      (6) must put in place a policy which states that should there is any indication of data theft related to customer authentication aspect, Bank must immediately replace customers’ authentication data.

b. Bank must write down and determine procedures ensuring that customer can not renounce any transaction (non repudiation) so that all transactions are credible, which include, amongst others:
   1) e-banking system has been designed to minimize the possibility of unintended transactions by rightful users;
   2) all party conducting transactions have been authenticated;
   3) data of financial transactions are protected from the possibility of alteration, and every alterations made are traceable. The process of recording financial transactions must be designed in the best manner possible to prevent

attempts of unauthorized alteration. Each attempt of unauthorized alteration need to be recorded (logged) and management of the Bank must be attentive to this matter;

4) implementation of methods ensuring the fulfillment of non repudiation principles, such as digital signature, Public Key Infrastructure (PKI). Keys used for encryption purpose must be maintained securely so that no party fully discerns the combination of such keys.

c. Bank must ensure the segregation of duties and responsibilities related to the use of the system, database and application of e-banking. Bank must ensure that dual control and segregation of duties are in place to further ensure performance of check & balance function. Bank must ensure segregation of duties between party who initiates/inputs data and the party who verifies the validity of such data. For example, in a banking application, each and every addition or alteration on database done by data entry operator, will only be effective with the approval of supervisor.

d. Bank must ensure availability of control on authorization and rights of access (privileges) appropriate for the system, database and e-banking application.

   All Bank's confidential archive and data can only be accessed by authorized parties. Bank's confidential data must be maintained securely and protected from the possibility of being compromised and modified by unauthorized parties.

e. Bank must ensure that certain methods and procedures are implemented to protect the integrity of data, records and information related to e-banking transactions with due observance to the followings:

   1) Bank must implement proper methods and techniques to minimize external threats such as viruses and malicious transactions, which include:
      a) software – providing virus scanning and anti virus software for all entry point and each computer system (desktop);
      b) software to detect intrusions (intrusion detection system);
      c) periodic penetration testing on internal and external network at least once a year.
   2) Bank must perform test on the integrity of e-banking transactions data.
   3) Bank must perform control function in order to ensure all transactions are conducted correctly.

f. Bank must ensure the availability of clear audit trail mechanism for all e-banking transactions, which includes the followings:

   1) Bank must maintain transaction log in accordance to Bank's data retention policy and in accordance to prevailing regulations, in order to provide clear audit trail as well as to support disputes settlement. Necessary transaction data should include at least customer's data, account numbers, types of transactions, time, location, amount of transaction;

2) Bank must notify customers when a transaction is being completed. When a transaction is being repudiated, such event must be documented and must have procedure of ensuing actions;
3) Bank must ensure the availability of audit trail function to enable detection of attempts and/or occurrences of intrusion that must be reviewed or evaluated periodically. If the processing system and audit trail function are the responsibility of a third party then such audit trail process must meet Bank's predetermined standards. Banks must have sufficient authorization to access audit trail maintained by the third party;
4) Bank must perform detection and monitoring on unauthorized/uncharacteristic transactions, i.e. using Intrusion Detection System (IDS) and Fraud Detection. Bank must also have procedures on handling problem or detected crime.

g. Bank must implement steps to protect the confidentiality of e-banking information. Security procedures shall be in accordance to the sensitivity level of the information.

   Bank must also have standards and control on the usage and protection of data when service providers/outsourcing have access to such data;

h. Bank must have a business continuity plan including an effective contingency plan to ensure the availability of e-banking system and services in continuity. Further regulations are available in Chapter VI regarding Business Continuity Plan;

i. Bank must develop prompt and proper incident response plan to manage, resolve, and minimize the impact of an incident, fraud, system failure (internal and external), that can obstruct the availability of e-banking system and services.

8.4.2.2. Principle of Security Control on Particular E-Banking Products

a. In providing banking services via e-banking, such as ATM and internet banking, Bank must also consider customer's comfortness and easiness in using the facilities, including the effectiveness of the display on e-banking menu, particularly on customer's instructions selection menu in order to avoid any error and loss in transactions;

b. To increase security, if necessary, Bank may predetermine requirement or limitation on transactions conducted via e-banking, to ensure the security and reliability of transactions, for example by requesting customers to register a third party beneficiary's account in mobile banking or by limiting the nominal amount on transactions through ATM and internet banking**;**

c. In e-banking which involves physical equipment like ATM, Bank must implement physical security control on equipments and rooms from the danger of theft, sabotage and other criminal actions by unauthorized parties. Bank must perform routine monitoring to ensure security and comfort of customers using e-banking service;

d. Bank must ensure the availability of security measures on data transmission aspect between Electronic Fund Transfer (EFT) terminal and the Host Computer, against risks of transmission error, network disturbance, unauthorized access, etc. Security measures shall comprise equipment control, monitoring on quality and accuracy of network equipments performance and transmission line, as well as monitoring on access to Controller software (Host-Front End);

e. Point of Sales (POS)/Electronic Data Capture (EDC) enable electronic fund transfer from customer's account to acquirer's or merchant's account for payment of a transaction. Transactions conducted via POS terminal located in shopping centrals or supermarkets generally involve a card-based payment instrument. POS may be provided by the Bank itself, or financial acquirer, technical acquirer or switching company. The party providing POS terminal must always increase the physical security around the vicinity of such POS terminal and on the POS terminal itself, amongst others by using POS terminal that minimize the possibility of interception on such POS terminal or in its communication network.

f. For mobile banking (m-banking) services, Bank must ensure the security of transactions by implementing the followings, among others:

   1) employ a SIM Toolkit with end-to-end encryption feature from hand phones to m-banking servers, to protect data transmission in m-banking;

   2) employ dual authentications, whereby Bank and customers can perform authentication process with digital certificate, Personal Authentication Message which helps customers to ensure that the party having transaction with them are the authorized parties (Bank, service providers).

g. For phone banking service, Bank must ensure the security of transactions, by implementing the followings, amongs others:

   1) this service shall not be used for transactions with high value or risk;

   2) all IVR conversations shall be recorded, including customer's phone number, transaction detail, etc;

   3) this service shall use reliable and secure authentication methods;

   4) the use of customer's authentication method such as PIN and password for financial transactions.

8.4.2.3. Customer Education and Protection

Bank must educate e-banking customers in realizing and understanding the risks involved in e-banking. Items need to be done by Bank comprise, amongst others:

a. For internet banking transactions, Bank must ensure that Bank's website has provided information that enable potential customers to obtain sufficient information about the Bank's identity and legal status before conducting any transaction. Such information are, including but not limited to, name and location of the Bank, identity of Bank's supervision authority, procedure in accessing customer service unit (call center) and procedure in filing complaints;

b. If Bank allows customers to open an account via internet, information regarding regulation on "Know Your Customer" must be available on Bank's website, amongst others, informing customers to be present and have an interview in the Bank in order to complete the process of opening an account;

c. Bank must ensure that protection on customer's data confidentiality is in place with to observance to prevailing regulations, and only accessible by authorized parties. Customers should also be given an understanding about Bank's internal regulations regarding customer's data confidentiality;

d. Bank must ensure that customer's data are not used for purposes other than ones authorized by the customers. In accordance to prevailing regulations on transparency of product information and the use of customer's personal information, Bank must obtain customer's approval prior to give the customer's personal information to service providers for marketing purpose. Protection on customer's data confidentiality must also be implemented in the event that Bank use outsourcing services;

e. Customer education shall comprise rights, obligations and responsibilities of all related parties. Education at least must be given when customers apply for e-banking service.

   Items need to be educated are, amongst others:

   1) the importance to keep PIN/Password secured, for example:
      a) keep PIN/Password confidential and do not disclose it to anyone including Bank's employee;
      b) change PIN/Password periodically;
      c) use PIN/Password that is not easy to predict (do not use personal information such as date of birth);
      d) do not write the PIN/Password;
      e) PIN for one product should be different from the PIN for another product.

   2) Implementation of prudential principles when using ATM, amongst others:
      a) examine the security of environment around the ATM before deciding to draw money;
      b) ensure that the money and the card are already taken before leaving ATM location.

3) providing information on how to secure customers' personal computer used to conduct transactions via internet banking.
4) Complaint procedure for troubles
5) Implementation of prudential principles in using mobile banking, for example:
   a) not to store PIN in telephone memory to prevent illegal duplication of sim card or PIN theft through redial function;
   b) employ methods to verify the authenticity of customers and/or Bank who came into contact, such as by using personal assurance message which basically are personal information submitted by customers to the Bank during registration, so customers and Bank can perform verification prior to conducting transactions.
6) In term of internet banking, it may be necessary to provide education about various methods of internet banking crime, such as:
   a) phising and other social engineering crimes;
   b) key logger and Trojan Horse Virus in various computer equipments commonly present in public places such as Internet Café, etc.

8.4.2.4. Cross Border Electronic Banking

Risk of cross border e-banking is mitigated by:

a. constructing effective risk management program for cross border e-banking activities. Prior to Bank introduce products and services of cross border e-banking, the management of the Bank should carry out proper risk assessment and due diligence to ensure that the Bank has properly managed existing risks. Apart from observing prevailing laws and regulations in Indonesia, Bank should also observe the prevailing laws and regulations in the country where the Bank intend to offer cross border e-banking service.
b. sufficient disclosure on the website or other information to enable potential customers to understand the Bank's identity, home country, Bank's supervision authority and approval/license obtained by the Bank, prior to conducting any business relation with such Bank.

8.4.2.5. Risk Management Related to E-Banking System and Service Operated by Service Provider

In the event that e-banking operational system is outsourced to other party such as switching company or ISP, Bank must determine and implement monitoring procedures as well as complete and continual due diligence to manage the relation of Bank with such service provider. For that purpose, Bank and the service provider of e-banking service must enter into agreement which regulates in detail rights and obligations, security aspect, and monitoring on service provider performance in accordance with the service level agreement. Further regulations on this matter are available in Chapter X – Guidelines of The Use of Information Technology Service Provider.

8.5 INTERNAL AUDIT

The purpose of audit on e-banking activities is to test the effectiveness of implementation of risk management on e-banking, as well as to ensure that the security control of such product is adequate in providing protection to customers. Audit on e-banking activities shall at minimum comprise evaluation on board and management oversight, assessment on implemented security program as well as review of compliance to regulations.

Implementation of audit on e-banking service shall at minimum refers to Chapter IX - Audit.

8.6. REPORTING OF PLAN & REALIZATION OF NEW E-BANKING PRODUCT

Each plan to issue transactional Electronic Banking product must be reported to Bank Indonesia at the latest 2 (two) months prior to the issuance of such, by using index 2.2.1. Development Plan of Electronic Banking Transaction. Requirement to report electronic banking product plan shall applies for each new product with different characteristics from existing products and/or which add or increase certain risk exposure to the Bank. This reporting requirement shall not apply for Electronic Banking products, specifically regulated in Bank Indonesia’s regulation regarding approval requirements of such products.

If the Information Technology used in operating Electronic Banking activities is provided by service providers, regulations on the employment of service providers shall also prevail, as regulated in Chapter X regarding The Use of Information Technology Service Provider.

“New Electronic Banking products” shall mean new products having different characteristics from existing products and/or which add or increase certain risk exposure to the Bank, such as internet banking and phone banking for deposit account customers.

Consequently, when a Bank only add types of service in existing e-banking products and the risks are not significantly increased, for example addition on payment facilities through e-banking from previously only capable of serving credit card payment to capable of serving electricity or telephone payment, such addition of payment service shall not be categorized as new product and therefore does not need to be reported.

However, when a Bank adds a service, from previously only capable of handling Indonesian rupiah transactions to capable of also handling foreign currency transactions, Bank must report such new product, because based on risk analysis, such transaction may increase market risks, legal risks, and other risks.

Subsequently, at the latest 1 (one) month after such activities effectively in operation, Banks must report the realization of such activity in accordance to the form of Fundamental Alteration Report in The Use of Information Technology by using Index 2.3.1. Transactional Electronic Banking Publishing Realization. The realization report must be complemented with reviews on the result of implementation (Post Implementation Review) by independent parties. New products and/or activities reported in Realization Report of Information Technology Fundamental Alteration Plan do not need to be reported in Report of New Product and Activity, as regulated in the regulation of Bank Indonesia regarding risk management of commercial Banks.

8.6.1. Report of Plan & Realization of E-Banking New Product

In the report of transactional e-banking Issuance Plan, Banks must attach:

a. evidence of readiness to operate e-banking which include at minimum:

1) readiness of organization structure including monitoring from the management;
2) readiness of policies, systems, procedures and authorization in issuance of e-banking product;
3) readiness of IT infrastructure to support e-banking products including but not limited to network structure, operating system, interface between e-banking system and the entire system;
4) the result of analysis and identification of risks attached to e-banking products;
5) readiness of risk management implementation particularly of adequate security control on e-banking products, amongst others to ensure the fulfillment of the principles of confidentiality, integrity, authentication, non repudiation, and availability;
6) the result of legal aspect analysis related to agreements between Bank and customers as well as other supporting parties, choice of law used in the event of dispute;
7) description of accounting information system including brief explanation on it's correlation to Bank's entire accounting information system;
8) customer protection and customer education program on the system and e-banking security technology.

b. The result of business analysis regarding new products projection for the next 1 (one) year, which covers at least:

1) existing market potential;
2) targeted market segment;
3) business competition analysis;
4) targeted customers;
5) cooperation plan with other parties;

6) targeted income.

c. Assessment result from independent parties to provide opinion on products' characteristic and sufficiency of product security as well as compliance to regulations and/or international best practices.

8.6.1.1. Assessment by Independent Party

Assessment result by independent parties as mentioned above is aimed to provide opinions on products characteristics and IT system security sufficiency related to such products, as well as compliance to prevailing regulations and/or international best practices such as ISO, IEC, COBIT, IT-IL.

Independent parties shall mean parties uninvolved in the designing and development of application system, as well as in making decision for implementation (go or no go).

Assessment result from independent parties outside Bank (Public Accountant Office, IT security consultant companies or such) is needed for transactional e-banking products issued for the first time such as transactional internet banking and transactional sms banking.

On the other hand, for additional features to existing e-banking products which may increase risk exposure, Banks may use internal parties to perform independent review.

For example:

a. ATM transactions, from unable to conduct overbooking to capable of doing so;
b. ATM transactions, from only capable of intrabank overbooking to be able to conduct interbank transfers.

Bank need to ensure that the external parties employed are competent and have an understanding on the products to be reviewed, especially from IT security aspect. In the event that Bank use an internal party to perform independent review, Bank must provide descriptions of duties and responsibilities of such party as well as its position in the organization structure of e-banking application development project.

8.6.1.2. Scope of Assessment by Independent Party

Bank must ensure that the reports submitted by independent parties regarding the readiness of Bank's IT for planned e-banking activities cover the assessment period, scopes, assessment methods, findings, recommendations, management response on the findings, as well as accomplishment target. The scope of the assessment comprises:

a. management's active monitoring;

b. sufficiency of e-banking system security policies and procedures to ensure the fulfillment of the principles of confidentiality, integrity, availability and non repudiation in each e-banking transaction;
c. sufficiency of implementation and monitoring on e-banking application system security prepared by the Bank, which comprises:
   1) implementation of application security, infrastructure (server, firewall and router) as well as e-banking system network;
   2) security to detect uncharacteristic transactions;
   3) availability of maintenance and review on audit trail log of transaction;
   4) satisfactory physical security on computer equipments and communication equipment related to e-banking products/services;
   5) security on bank's internal network for protection from external attacks;
   6) security on data and database of e-banking transactions.
d. Business Continuity Plan and incident response management;
e. employment of IT service providers as e-banking operator;
f. review on risk analysis of new e-banking products, which at minimum covers strategic risks, security risks, legal risks, reputation risks;
g. education and customer protection program including prudence in opening account and conducting transactions via e-banking.

CHAPTER IX
INFORMATION TECHNOLOGY INTERNAL AUDIT

9.1. INTRODUCTION

Effective Internal Control (SPI) is an important component in Bank's management and become the base of clean and safe Bank's operations. An effective SPI assists Bank's management to protect Bank's assets, guarantee~~ing~~ the availability of accountable financial and managerial report, increase Bank's compliance to regulations, as well as to decreasing the risks of losses, discrepancies and violations of the aspect of prudence.

The use of Information Technology (IT) facilities other than increasing the Bank's capability of carrying out operations, also contain risks of possible losses, both ~~of~~ financial or non-financial. Therefore SPI is required to be implemented as a way to ~~of~~ minimize the losses. The internal audit function as a part of SPI, is responsible to evaluate IT operation independently and objectively to increase the efficiency and effectiveness of risk management, internal control and good corporate governance.

This guideline is meant to be a reference for Banks in IT internal audit impelementation.

9.2. DUTIES AND RESPONSIBILITIES OF ~~THE~~ MANAGEMENT

Information Technology internal audit is a part of Internal Audit Work Unit (SKAI) independent from operational duties of the organization or the function. In carrying out its activities, internal audit must obtain management support formalized in an Audit Charter. Audit Charter at least contains information regarding positions, purposes and scope of work, duties, authorization and responsibilities of internal audit. The Audit Charter also contains independency statements on operations from auditee and statements that each of Bank's activity must be included in Bank's internal audit scope.

The success of IT internal audit requires the support and commitment from the Board of Commissioners, Audit Committee and Directors. Those parties need to ensure cooperation between the management of IT and the management of IT audit unit. Beside that, those three parties also need to ensure that the implementation of control, procedures and standards are done by IT working unit and IT users working unit. Also need to be ensured is that the process of audit includes attempts of verification and monitoring on the implementation of control and the carrying-out of procedures and standards adequately, punctually and independently.

9.2.1 Internal Audit Working Unit Function

In order to IT internal audit to be effective and assure data integrity and support Bank's operational continuity, Internal audit working unit at least carries out the following:

a. arrange and update work references which at least include the set standards of assessment procedures, work sheet and reports of examination result;
b. identify IT risk area that will become the focus of audit;
c. evaluate the function and sufficiency of internal control in Bank's information system;
d. ensure the implementation of the principles of IT confidentiality, integrity and availability;
e. evaluate the effectiveness of IT operation planning and monitoring by IT working unit and IT users working unit;
f. evaluate Bank's IT compliance to internal regulations, Bank Indonesia regulations and state regulations as well as international best practices (such as ISO, IEC, COBIT, IT-IL, Capability Maturity Model);
g. recommend on remediation alternative to handle the deficiency of aspects related to IT especially in the field of security;
h. perform monitoring on the ensuing actions on the audit result;
i. act as sources of information in the aspect of control where Banks perform IT development, such as application developments.

9.2.2 Roles of the Board of Commissioners

The main duty of commissioners related to the use of IT amongst others are evaluating audit planning and organizing, ensuring audit is carried out with sufficient frequency and scope, as well as monitoring the follow up actions on the audit result.

9.2.3 Roles of Directors

Roles and responsibilities of Head Director are, amongst others:

a. determining references, systems and procedures of internal audit;
b. ensuring the carrying-out of IT audit function by competent and independent resources;
c. ensuring that human resources as of IT internal auditor are adequate and qualified as well as have had necessary IT education and training continuously IT rapid trends;
d. agreeing on audit plans before it is implemented.

9.2.4 Roles of Audit Committee

Roles and responsibilities of Audit Committee :

1. monitor and evaluate IT audit plan and implementation with sufficient frequency and scope;

2. monitor follow up actions on audit result by the directors on Internal Audit working unit findings, public accountant and Bank Indonesia supervision.

9.3. IT AUDIT REFERENCE

Banks need to have a written IT audit guideline agreed by the directors. The complexity of the IT audit guideline is adjusted to the purpose, business policy, magnitude and complexity of the Bank.

IT audit guideline contains amongst others, policies and procedures necessary for the function of IT internal audit and policies and procedures of conducting internal audit by other parties when necessary. Said guidelines other than being used as facilities to achieve effective and efficient audit result, are also guidelines in assessing the performance of IT internal audit. Said guidelines must include policies, procedures and standards for every steps in audit cycles.

9.3.1. Audit General Policy

IT internal audit guidelines at least include general policies regarding:

a. statements of IT internal audit visions and missions;
b. organization structure and report system;
c. risk assessment process which illustrate inherent risks in each of IT working unit and IT user working unit, which is updated periodically and become a base for IT internal audit planning;
d. determining frequency and schedule of audit that will be implemented for IT audit as minimum. Audit on the IT operation must be planned and conducted at least once a year on aspects related to IT in accordance to requirements, priority and results of Bank's IT risk analysis. On the other hand, for the application of Core Banking, the entire module should be examined by IT internal audit at least once in 3 (three) years;
e. procedures of IT internal audit for every activity requiring IT audit.

9.3.2. Audit Planning

Bank's Internal audit working unit must have annual audit planning with the extent of audit based on risk profile of each activity related to IT in both IT working unit or IT users working unit. In assessing risks, IT internal audit at least carries out the following:

a. identifying data, applications and operation systems, technologies, facilities and personnel;
b. identifying business activities and processes which use IT;
c. considering priority scale based on the impacts and possibilities of risks on business activities related to IT.

Audit planning must have approval from President Director or Head Director.

9.3.3. Audit Conducting

In conducting annual audit plan, audit working program (AWP) must be arranged for every audit assignment, which includes at least:

a. organization, authorization and obligations of auditor;
b. scope of audit in accordance with the result of risk assessment;
c. audit purpose, schedule, number of auditor, funds and reports;
d. outlines of audit technical steps necessary to achieve the purpose of audit.

In doing its duties, IT internal audit must consider data confidentiality aspects and information obtained. Bank's Internal audit working unit must consider AWP flexibility so as to be suitable and complemented in accordance with identified risks.

Audit findings must be accompanied by evidences and assessment work sheet which are well documented. For that, audit guidelines must be complemented with standards of work sheet, report content and form of audit result, documentation and distribution as well as monitoringon the follow up actions.

IT internal auditor need to play a role in the main applications development, establishment, conversion and testing, although not as the determiner of how the applications being developed or established can or can not be implemented, but to participate as a source in the aspect of control especially regarding security standards necessity. This role is needed for the IT auditor to safeguard the independency and objectivity in the examination which is going to be done when the application system has been implemented.

9.3.4. Reporting

Report of the IT Internal Audit result is arranged based on report forms supported by audit work sheet determined in the guideline of internal audit. Said report is a facility for the management to assist the assessment on quality and performance of IT working unit, as well as providing its restoration suggestions. Report of IT internal audit result must be submitted to inspected working units. Beside that, said report is submitted promptly to the Head of Director and the Board of Commissioners / Audit Committee and a copy to the Director of Compliance. IT internal audit report is also submitted to Bank Indonesia as a part of the Report of Conducting and Key Points of Internal Audit Result, as regulated in the regulations regarding the conduction of internal audit function standards.

9.3.5. Audit Follow Up Actions

Audited parties must give feedback on the result of the assessment and if the findings need to be followed up then the Audited parties must present their commitment and completion duration target. Furthermore, Internal audit function must periodically monitor the conduction of the audited party's commitment on the result of the assessment and verify the correction conducted.

Internal audit must maintain documentation on the result of said follow up actions. The report of follow up actions on assessment result is submitted to the Head Director and the Board of Commissioners/Audit Committee and a copy to the Director of Compliance.

9.4. IT INTERNAL AUDIT CONDUCTED BY OTHER PARTIES

When there is a capability limitation of internal audit function on Bank's Information Technology, then the conducting of internal audit function can be done by external auditor such as Public Accountant Office, Independent IT Audit Organization or the main office internal auditor for banks under foreign banks. The use of external auditor to perform the internal audit function on Bank's Information Technology does not decrease the responsibility of the chief of Bank Internal Audit Working Unit on audit findings and follow up actions.

The use of other parties as the IT internal auditor as mentioned above must consider the complexity of product and business scale of the Bank. The conducting of IT internal audit by external auditor remain considering the aspect of competency (amongst others are adequate knowledge and experience) and independence as well as based on an employment contract. Even though the conducting of internal audit is handed out to external auditor but the IT audit procedures used must remain referring to the policies and procedures of IT audit of the Bank.

9.5. INTERNAL AUDIT ON OTHER PARTY SERVICES

To ensure the use of Information Technology organizers service providers to support Bank's capability of managing its business effectively, those said activities are also covered in Bank internal audit scope. The function of Bank internal audit must ensure the control operated by service providers, and perform tests on the effectiveness of said control. Banks must ensure that the agreement with the service providers include the clause of right of access for Bank internal auditor and for service providers acceptance to be audited by Bank internal auditor. Said provided access must be given for logical and physical means.

9.6. IT INTERNAL AUDIT REVIEW

Banks must review the internal audit function on the use of Information Technology for at least 3 (three) times a year. Said review must use the service of independent external parties that work independently. What is meant by independents are third parties which do not have any financial, management, stock ownership relation or other relation that affect their ability to act independently. What is meant by work independently is the ability to express points of view as well as thoughts in accordance with their profession, by not taking sides on other party's interest.

Said review should at least asses the result of internal audit working unit and compliance to regulations related to Internal Audit Standard for Banks and to risk management including risk management on the use of information technology as well as other regulations. The result of the review accompanied by correction suggestions is reported to Bank Indonesia and is a part of the report of internal audit working unit (SKAI) review as regulated in the regulation regarding conduction of internal audit function standard.

CHAPTER X
THE USE OF INFORMATION TECHNOLOGY SERVICE PROVIDER

10.1. INTRODUCTION

In order to increase the effectiveness and efficiency in achieving strategic aims, Banks can use IT service providers. What is meant by using information technology service providers is using the service of other parties in carrying out activities of Information Technology which then cause the Bank to become dependent on services given in continuity and/or in certain periods.

The use of IT service providers can affect the Banks' risks, amongst others operational risks, compliance risks, legal risks and reputation risks that can arise because of the failure of service providers in providing services, violation on security or inability to abide by valid law and regulations. To ensure that Banks run their business appropriately and securely, IT operations conducted by service providers also become the object of regulation and monitoring of Bank supervisory board. Bank Indonesia as Bank supervisory board has the authorization to observe all activities and financial records of a Bank conducted by the Bank itself of by other parties. Therefore, Banks assessments and monitorings must not be obstructed by transitions of Bank's operational functions to other parties.

10.2. RESPONSIBILITY OF THE MANAGEMENT

The Bank's management is fully responsible for ~~on~~ the implementation of risk management on every activities related to the use of service providers in the carrying-out of Bank's IT. If a Bank outsourced its IT operations to a third party, the accountability remains on the Bank even though the day-to-day responsibility has been transferred to the service provider. And so the responsibility of the management does not disappear or reduced with the use of IT service providers. For that, the Bank's management must manage the risks caused by said activities effectively by, amongst others:

a. understanding the entire the risks that could arise from outsourcing the IT operation to third parties, either partially or entirely;

b. the use of IT service providers gives a consequence of Banks sharing sensitive information to service providers, and so the management must evaluate the capability of service providers to safeguard the security level to at least the same or to a tighter level than Bank's security standard. For that also, monitoring and surveillance must be done adequately to ensure the sufficiency of protection on previously mentioned information security;

c. evaluating potential service providers based on the scope and critical factors of the services delivered by service providers;

d. considering several alternatives in selecting of different service providers if the activities to be handed out are important;
e. perfoming review in assessing the reliability of service providers relating to the performance, reputation and the continuity of service providing, in choosing Bank's service providers alternatives;
f. ensuring that Banks have sufficient skills to observe and manage cooperation with service providers including implementing effective control;
g. ensuring that every cooperation with service providers are well managed by the Bank and can meet the requirements of Bank operations and allign with Bank strategic plan;
h. ensuring that Banks have documentation related to activities of IT service providing, amongst others, procedures, assignments/responsibilities and report mechanism;
i. performing continuous monitoring on Bank activities conducted by other parties to handle identified risks and to evaluate risk changes occurred in the time of IT operations compared to the initial assessment;
j. performing reviews on contracts/agreements periodically to recognize the accordance with Bank's requirements and most recent condition;
k. for the use of IT services with high risk exposure (based on the result of Business Impact Analysis) such as the carrying-out of Data Center and Disaster Recovery center, Banks should use legal consultant since the beginning of the process of the plan to use the service of other parties, to study the proposal submitted by service providers and to assist in preparing the agreement so as to enable Banks to understand the existing legal risks and then implement necessary mitigation on risks.

When outsourcing the IT operations to third parties, Directors are responsible to:
a. determine policies and procedures to be used by the Bank in evaluating the risks and impacts from the use of other parties already present or going to be used;
b. govern the authorization of agreements of using IT service providers in accordance to the types of risk and its impacts;
c. develop policies and procedures of proper and responsive risk management on the use of the service of a third party in accordance with its characteristic, scope and complexity;
d. ensure periodic review on relevancy, security, strategy reliability and sufficiency of agreements.

When outsourcing the IT operations to third parties, the IT highest rank officer is responsible to:

a. implement policies and procedures of proper and responsive risk management on the use of the service of a third party in accordance with its characteristic, scope and complexity;
b. ensure effectiveness of periodic review on policy and procedure;
c. ensure that the contingency plan is arranged and tested based on scenarios with consideration on various types of disturbance;
d. ensure review and audit by independent parties on the compliance to the policies.

10.3. POLICIES AND PROCEDURES

10.3.1. General Policy

Banks must have guidelines regarding the outsourcing of IT operations to third parties, which at least govern the following:

a. standard procedure for vendor/third party selection;
b. standard content of contract agreement with service providers;
c. security baseline standard, accuracy and integrity of technology system which must be fulfilled by service providers;
d. security and confidentiality of information especially regarding customer's information;
e. evaluation of risks and impacts from the use of other party services;
f. other items obligatory for Banks in the carrying-out of IT by other parties in accordance with rules regulated in the Regulation of Bank Indonesia regarding Implementation of Risk Management in the Use of IT.

10.3.2. Process of Service Provider Selection

10.3.2.1. Requirement Definition

The outlining of business requirements on the use of services by other parties must be done before Banks decide to use the third party services, through, amongst others:

a. specific identification process about functions or activities to be handed over to service providers;
b. risk assessment process which can arise from the handing over of said functions or activities; and
c. establish standard to be used to identify the measurement of adequate control.

This phase must produce a document with detailed illustration regarding Bank's expectation on the services conducted by service providers. The content of the document includes several components as follow:

a. scope and characteristics of the services, technology being used and support for customers;
b. standard and level of services including the availability and performance, change management, service quality, security, business continuity;
c. minimum characteristics that must be met by service providers to be used, such as experience, architecture of technology and system, process control, financial condition, reference about reputation;
d. monitoring and reporting including criteria to be used in the monitoring and reporting for Banks or for service providers;
e. requirements to be met from the standpoint of the system, data or personnel training at the time of transition or migration to the system provided by service providers;
f. duration of ~~a~~ contract, termination and minimum content of ~~a~~ contract;
g. contract protection on responsibilities, such as restriction of responsibility and reimbursement as well as insurances.

If the carrying-out of the previously defined activities or functions is considered to be conducted by a party related to the Bank, then the management of the Bank must ensure that the preparation will not be different if it is conducted by a party unrelated to the Bank.

10.3.2.2. Request for Proposal from Service Provider

The process of service provider selection begins with a request for proposal from service providers. The presented proposal must explain in detail the Bank requirements such as the scope and the type of assignment to be done, expectation level of service production, completion duration, measurement of assignment and its control, security and business continuity.

When Banks evaluate the proposal, there is a possibility of discordance with the Bank requests. And so Banks must evaluate the differences and their impacts to the objectives and services expected. There are among others, Banks must study the policies the of service provider related to the importance of Bank IT audit because access of internal, external or Bank Indonesia auditor must not be decreased. And so the necessary data and information from the carrying-out of IT are still obtainable promptly every time it is needed even though the IT used by the Bank is not carried out by the Bank itself. For that, letters of declaration must be included in the proposal presented by service providers. After that, if the proposal has met the requirements or suitable with the requirement definition, then Banks conduct conclusion negotiation with the service provider before the establishment of contract.

10.3.2.3. Service Provider Due Diligence

Due diligence is necessary to asses the of financial condition, reputation, technical capability, operational capability, future development strategy, ability to follow market innovation and have good reputation in banking industry. And so Banks are certain that service providers are capable of fulfilling the Bank requirements. In the time of due diligence, Banks must conduct evaluation and assessment on information related to the service providers, which include, amongst others:

a. company's existence and history;
b. company's qualification, background and owner reputation;
c. reference from other companies using the same services of the service provider;
d. financial condition including review on audited financial report;
e. capability and effectiveness of service providing, including post sale support;
f. technology and system architecture;
g. internal control environment, security history and audit scope;
h. compliance to existing law and regulations;
i. trust and success in relationship management with sub contractors;
j. insurance;
k. ability to provide disaster recovery and business continuity;
l. implementation of risk management;
m. report of independent party assessment result.

Due diligence by the Bank during the process of selection must be well documented and repeated periodically as a part of the process of monitoring and control. In conducting this due diligence periodically, Banks should consider existing changes or development during the time period since the last due diligence by using the most recent information.

10.3.2.4. Service Provider Selection

In determining service provider to carry out Bank's IT, then Bank must consider the following:

a. because the use of service provider does not reduce the responsibility on Banks in implementing risk management then Banks must evaluate the implementation of risk management by service providers;
b. because Banks must be able to conduct monitoring on Bank's activities carried out by Information Technology service provider, then Banks must ensure that the reports necessary to monitor the performance of service provider are adequate, including if the monitoring program is actually required;
c. cost and benefit analysis being done for every alternative to be selected must be in deep and fulfill the time duration of service planned in accordance with IT Strategic Plan & Business Plan;

d. in studying every alternative, the management of the Bank must ensure that the Information Technology work unit in the Bank present their opinions and analysis results;

e. the service providers implement the principle of IT control adequately including physical security and logical security. For the carrying-out of Data Center, DRC and IT-Based Processing, it must be ensured that service providers can submit the latest result of audit on Information Technology by an independent party;

f. in order to monitor and evaluate the reliability of service providers periodically, that relates to performance, reputation and continuity of service providing, Banks can obtain said information from various source including annual reports of said IT service providers;

g. Banks must study whether the database are accessible by Bank Indonesia, at timely manner for both the latest data or past data;

h. If the IT service provider is related to the Bank, Banks must still conduct selection process. Selection documentation must be able to show that considerations abide to the “arm’s length principle.”

10.3.3. Service Provider Agreement

After choosing a service provider company, the management establishes a written agreement with the service provider. The content of the proposal as required in the previous process should be considered in this process. The agreement is a legal document that defines every aspect of the relation with service provider and becomes the main control tool.

10.3.3.1. Arrangement of Service Provider Agreement

Minimum items that must be regulated in the contract include, amongst others:

a. scope of work/service;

b. cost and duration of contract agreement;

c. rights and obligations of Banks and service providers;

d. security guarantee and confidentiality agreement, especially customer’s data. Data are only accessible by the data owner (Bank);

e. Service Level Agreement (SLA), contains of performance standard such as agreed service levels and performance target;

f. must be determined that SLA remains valid in the event of the changing of the ownership of Bank or service provider;

g. reports of the monitoring result on service provider’s performance related to SLA;

h. limitation of risks sustained by Banks and service providers:

1) risk of changes on the scope of contract;

2) changes on the scope of business and service provider company organization;

3) changes on the aspect of law as well as regulations;
4) aspect of law including copyrights, patent and trademark;

i. subcontractor, if service providers subcontract parts of their activities the Bank's agreement must in writing;
j. provision of on-line communication facilities, security on data access and transmission to and from Data Center, Disaster Recovery Center, and IT-based Transaction Processing;
k. clear regulations regarding backup, contingency, record protection including hardware, equipment, software and data files, to ensure the continuity of the carrying-out of IT;
l. regulations regarding security in the submission of necessary source document to and from Data Center, Disaster Recovery Center, and IT-based Transaction Processing. The responsible parties should have adequate insurance coverage;
m. willingness audited by Bank's internal, Bank Indonesia or external parties assigned by the Bank or by Bank Indonesia, and the availability of information for the purpose of assessment, including rights of logical and physical access, on data managed by service provider;
n. service provider must submit technical document to the Bank in relation with the service conducted by the service provider, amongst others, IT process flow and database structure;
o. service providers must report every critical occurrence that can cause financial losses and/or disturb Bank's operations;
p. specifically for the outsourcing of Data Center, DRC and IT-based Processing, service provider must submit the latest financial report to the Bank, which is audited annually, and the report of periodic assessment result by an independent party on IT facilities which are as the object of agreement;
q. responsibilities of IT service providers in providing human resources with relevant qualification and competence in accordance with the service provided, so as to ensure Bank's operations;
r. plans of training for human resources, including number of employee to be trained, forms of training or required costs. Service providers must conduct knowledge transfer to the Bank, so there will be personnel of Information Technology work units that understand the IT used in the Bank especially IT process flow and database structure from the application system provided by said service providers;
s. ownership and license;
t. guarantee that service providers will provide support and maintenance services to Banks during a certain period of time after the implementation;
u. end/termination of contract including if it is requested by Bank Indonesia;

v. penalties on vague reasons on the cancellation of contract and violation of contract;
w. compliance to existing law and regulations in Indonesia including the dispute/conflict resolution.

10.3.3.2. Special Clause

the contract between Banks and service providers, must contain special clause regarding the possibility of changing, making new agreements or taking over activities of the service providers or termination of agreement before the end of the duration of the agreement. The clause also applies subject to the request of Bank Indonesia if necessary, due to BI's role as banking supervisory authority. Banks must be able to measure the risks and efficiency of the carrying-out of IT which is handed over to service providers so that Banks can promptly notify if there are certain conditions as the following:

a. declining performance of Bank's activities conducted by service providers which can significantly affect Bank's business;
b. the level of solvability of service providers is not adequate, in the process to liquidation or declared bankrupt by a court of law;
c. violations on the regulations of Bank's secrecy and customer's personal information; and/or
d. conditions which cause Banks unable to provide necessary data in timely manner for an effective monitoring by Bank Indonesia.

If Banks discover the issues mentioned above the Banks must conduct the following:

a. report to Bank Indonesia within 3 working days at the latest after the abovementioned conditions are acknowledged by the Bank;
b. decide the ensuing actions to be taken to resolve problems, including the termination of the use of services if necessary;
c. report to Bank Indonesia immediately after the Bank halts the use of the service before the end of the time duration of the agreement.

To maintain the continuity of Bank's business when halting the use of services before the end of contract, Banks must have adequate and tested contingency plan.

10.3.4. Service Provider Outside Indonesia

In principle, Data Center and/or Disaster Recovery Center should be conducted domestically. If the previous process of requirement definition phase conducted by Banks stated that Banks decide to use the service of other parties, resulting the need of using out of Indonesia service provider to conduct Data Center and Disaster Recovery Center, then Banks can consider the use of IT Services Provider out of Indonesia. One issue that must be understood by Banks planning to use the service of service provider outside Indonesia is that said plan must not be an attempt to avoid/obstruct monitoring or assessment by Bank Indonesia. The same as with the use of domestic IT service provider, the use of IT service by foreign parties or parties located outside Indonesia, must go through the same procedures, starting with due diligence, service provider selection, the making of contract and monitoring, but because there is a differences of jurisdiction then there are other prerequisites to be considered by Banks. Banks that are going to outsource Data Center, Disaster Recovery Center and/or Technology-based Transaction Processing out of Indonesia must first obtain the approval from Bank Indonesia. The approval includes the outsourcing of IT activities to be conducted at the Bank's office, bank's parent office or Bank's business group office out of Indonesia. On the other hand, the use of out of Indonesia service providers for other IT activities such as development of program and application used by Banks as well as maintenance of hardware & software, can use the service of foreign service providers without first obtaining the agreement of Bank Indonesia, as long as banks abide regulation in Chapter 18 PBI Implementation of Risk Management in The Use of IT, and regulations in this guideline.

To obtain the approval from Bank Indonesia, banks has to fulfill requirements as mentioned before and also fulfill the following:

a. Banks must conduct analysis and feasibility study on government policies, condition of politics, social, economy and law in countries where the IT is carried out. Beside that, bank needs to analyze its ability to monitor the service providers effectively, Bank's ability to conduct Business Continuity Plan and early termination;
b. country risk analysis which shows that there are no significant impacts from the location out of country, including in the event of dispute with the country where the service provider is in;
c. Banks must conduct assessment on local regulation in countries where service provider is established that required the service provider to provide information disclosure on customer's data in a certain issue or case, eventhough there is customer's data confidentiality clause in the contract agreement;
d. In principle Banks can only make agreements with other parties which operate in a jurisdiction which generally support the clause and agreement of confidentiality. And so Banks must ensure that the written agreement with service providers also include the choice of law, and Banks understand the possible impact from the choice of law to resolve disputes or legal problems in the future;
e. to be able to provide all necessary data in the event of an monitoring by Bank Indonesia, Banks must ensure that the database structure of every application used is owned by the Bank and stored in the Bank's office in Indonesia and there

are bank's officers inside the state which understand the database structure including technical reference of said database. Therefore Banks must ensure the placement of Data Center out of Indonesia does not obstruct the attempts to observe and reconstruct the Bank's activities inside the state (such as from accounting, accounts, and documents) in timely manner;

f. Banks can not place Data Center in a jurisdiction where access to information by Bank Indonesia or by other parties appointed by Bank Indonesia to act on behalf of Bank Indonesia on Data Center and its service provider, can be obstructed by legal or administrative restriction;

g. Banks must conduct a review on how the outsource of Data Center, Disaster Recovery Center and/or Technology-based Transaction Processing out of Indonesia enables access for Bank's auditor from internal, external or Bank Indonesia to obtain necessary data and information from the carrying-out of IT promptly whenever necessary;

h. Banks must notify Bank Indonesia if there are authorities out of Indonesia which request access on information about Bank's customers or if there arise a situation where the right of access of the Bank or of Bank Indonesia to obtain information and documents is restricted or refused;

i. if in the future the obstructions occur in conducting assessment on the carrying-out of Data Center, Disaster Recovery Center and/or IT-based Transaction Processing out-of-state previously mentioned, Bank Indonesia has priviledge to order the termination of the service provider agreement;

j. the assessment by Banks regarding cost & benefit must shows that the benefits for the Bank exceed the costs changed by Bank's provider/group/parent, including the potential of increasing quality of service to customers;

k. the assessment by Banks must include product development and human resources planning. Banks are required to improve capability of Bank's human resources, in the aspect of IT usage or in the aspect of business transactions or offered products even though the carrying-out of IT is located out of Indonesia;

l. if a Bank is a Foreign Bank Branch Office or a Bank owned by Foreign Financial Institution, then the Bank must submit in the approval request letter the following:

   1) Letter of Declaration from out of Indonesia financial institution supervisory authority that the IT service provider is object to their supervision;
   2) Letter of Declaration of home supervisor does not object Bank Indonesia intention to examine the carrying-out of Data Center and/or Disaster Recovery Center;
   3) Letter of Declaration stating that the Bank will periodically submit the result of assessment by the Bank's office out of Indonesia on the implementation of risk management to service providers. This Letter of Declaration include the planned duration;

4) the result of the assessment by the Bank's office out of Indonesia on the implementation of risk management by service providers.

m. especially for the plan to hand over IT-based Transaction Processing (activities of additions, deletions, changes and authorization on data done on application systems used to process the transactions) to other parties out of Indonesia, it needs a study which can help the Bank in fulfilling other additional prerequisites, which are:

   1) consider the aspect of protection on customers;
   2) activities are not related to inherent banking functions of which are savings, limited deposits, deposits or credits (except credit card). Included here are the creating of an account and maintenance of customer's personal information master file;
   3) financial administration supporting document on the transactions conducted in the Bank's office in Indonesia can be maintained in Indonesia;
   4) business plan which shows the attempts to increase the role of Banks in the economy of Indonesia.

   Request for approval must be submitted within 4 (four) months at the latest before changes effectively deployed, and the approval or the refusal will be given by Bank Indonesia within 3 (three) months at latest after requested documents are received completely. Other than the abovementioned prerequisites, Bank Indonesia could ask for additional prequisites from the Bank and/or conduct further assessment. The requirement depends on the impact of the use of IT service providers on the Bank, and the level of conviction on submitted documents.

10.4. RISK MANAGEMENT PROCESS

10.4.1. Risk Assessment

The use of other parties' service in carrying-out Bank's IT can contribute to several types of risk, which are:

a. Operational Risk – inability of service providers to fulfill the contract;
b. Legal Risk – legal uncertainty in conflicts with service providers and/or third party, and/or customer's allegation on an abuse of customer's data by service;
c. Reputation Risk – customer's dissatisfaction from the inability of service providers to fulfill the SLA;
d. Strategic Risk – discordance of the IT used by the Bank with the Bank's objectives, and strategic plans to achieve the objectives;
e. Compliance Risk – Bank's inability to fulfill existing regulations;
f. Country Risk – condition in a foreign country which can affect the ability of service providers in fulfilling standard of service providing.

In conducting risk identification, measurement and surveillance, Banks must always consider these three factors:

a. related to activities and functions carried out by service providers including the sensitivity of data being accessed, protected or controlled by service providers, transaction’s volume, and the level of importance of the activities and functions on Bank’s business;
b. related to service providers, such as financial condition, competency of the workforce, management and workforce turn over, experience of service providers, professionalism;
c. related to the technologies being used, including reliability, security, availability, and timeliness as well as the ability to follow technology development and regulation changes.

10.4.2. Risk Mitigation

Based on the PBI Implementation of Risk Management in The Use of Information Technology, Banks remain responsible for every implementation of Bank’s risk management. And so Banks must conduct risk mitigation for every weakness and/or violation of security policies and procedures as well as risk potency which can disturb the continuity of the carrying-out of IT, in the Bank or in the service providers.

10.4.2.1. Business Continuity Plan (BCP)

Banks must ensure that the risk of dependence to service providers can be mitigated so Banks are still able to run their business when the service providers fail to deliver on its services, relation termination or in the process to liquidation. Possible risk mitigation by the Banks includes:

a. ensuring that service providers have BCP according to the type, extent and complexity of the activities/services given;
b. actively obtain guarantee of the readiness of BCP of service providers, such as from periodic testing on BCP;
c. having the agreement to store source code program in the premise signed by both parties (escrow agreement) for applications with high risk exposure, if Banks do not own the source code of an application program conducted by service providers;
d. if the source code is not owned by the service providers, then service providers must give a guarantee to the Bank, that the continuity of the applications is supported by software developer principal.

To ensure the function and the effectiveness of BCP, Banks must arrange and conduct testing on BCP periodically, completely and include significant issues based on the types, extent and complexity of the activities conducted by service providers.

Beside that, service providers must conduct testing on their DRP in the service provider itself for the system or facility of IT or the transaction process which is being carried out without involving the Bank. The result of the service provider's testing on DRP is used by the Bank to update Bank's DRP or BCP.

10.4.2.2. Other Risk Management

Even though Banks or service providers have used advance systems, there remain the possibility of inside discrepancies, for example are human errors, weak procedure implementation as well as employee theft. Banks must ensure the presence of basic security control to mitigate the risks which include the following:

a. service providers must investigate the background of their employees because attacks from the inside are more difficult to prevent;

b. avoid the possibility of orphan accounts used for transactions. Password & e-mail from resigned employees must be deleted immediately;

c. physical environment of service providers or of Banks must be ensured of being secure, such as through the monitoring of people going in and out of a room, or from the possibility of flood and fire;

d. electronic environment of service providers or of Banks must be ensured of being secure all the time;

e. security procedures are updated periodically so as to abide to existing regulations and in accordance with best practices;

f. create groups conducting intrusion detection periodically from inside the Bank or by hiring professionals. Review their advance and ensure that the standards are implemented adequately;

g. ensure that the obligation of service providers to conduct security control on all information technology facilities being used and on processed data as well as produced information, has been written in the agreement;

h. ensure that before the agreement is signed, service providers has understood it and able to provide the necessary security level for each type of data based on the data confidentiality sensitivity;

i. make an effort so the cost expended for security is balanced with the necessary level of security and in accordance with Bank's tolerable risk level.

10.5. INTERNAL CONTROL AND INTERNAL AUDIT

10.5.1. Review/Monitoring

Banks must have monitoring program to ensure that service providers have conducted their assignment/providing services in accordance to the contract. The resources to support this program are varied depend~~ing~~ on the criticality and complexity of the system, process and service done by other parties.

Banks must conduct pre- and post-review of other service providers to ensure that the policies and procedures of the Bank's risk management have been done effectively.

Furthermore, review on performance and achievement of Service Level Agreement (SLA) are conducted periodically which is then documented in the form of a report. Monitoring must be conducted on the annual report of the service provider assessment.

10.5.2. Internal Audit

Banks must conduct the function of audit on service providers, by Bank's internal audit or external audit by an appointed party. If a service provider provides services to more than one Bank, then the service provider is able to appoint an independent IT auditor to conduct audit on the services given to each Bank. The result of the assessment done by an independent IT auditor is for the interest of each Bank so therefore the Bank's Internal audit function to remain responsible on the audit result and must ensure the accordance of audit with the Bank's audit policies and procedures.

The scope of audit is in accordance with the extent of assignments/services as written in the agreement contract. Audited area such as, amongst others, IT systems, data security, internal control frameworks and business contingency plan.

Banks must ensure that Bank Indonesia or any other party assigned by Bank Indonesia, has the right of access to service providers and Banks to obtain records and documents of transactions, as well as Bank's information stored or processed by service providers as well as right of access on reports and findings of audit on service providers related to the services given to the Bank.

GLOSSARY

***1. Acquirer*:**
Banks or institutions beside banks which conduct payment tools by using cards which can be in the form of financial acquirer and/or technical acquirer.

2. *Access*:
Entrance. An attempt to open a communication line with a certain hardware or software, such as modem used to open internet access. Said hardware or software other than to provide data are also used to accept data to be stored.

3. *Accountability*:
A mechanism to assess the responsibility on making decisions and actions.

4*. Administrator Log*:
Files in a system which store information about administrator activities.

5. AES (*Advanced Encryption Standard*):
Encryption standard based on the block cipher algorithm with a certain block's length (128 bit) and variable key's length (AES-128, AES-192, AES-256). AES is considered as the replacement for DES.

6*. Agile Software Development*:
Is a technical framework of system development which concentrates on repeating development in a project cycle (SLDC), such as planning, requirement analysis, design, development, testing and documentation.

7*. Arm's Length Principle*:
A cooperative principle of normal means with mutual benefits where each party to make a cooperation agreement has the same bargaining power even if the service provider is the related party.

8. *Automated Teller Machine* (ATM):
A computer terminal/machine used by a Bank which is connected to other computers through data communication which enables Bank's customers to store and retrieve money in the Bank or conduct other banking transactions.

9*. Audit Trail*:

Files in a computer that store information about user or computer activities which is stored chronologically, and can be used for audit or trailing.

10. *Authentication*:

Ability from every party involved in a transaction to test the genuineness of other parties.

11*. Back Door*:

A methods to pass normal authentication or a secure remote access from a computer on the accessing of a system but unidentifiable from a normal inspection.

12*. Backup*:

Copies of original documents or auxiliaries of the main machine which can be used in the event of disturbance on the main machine. Backup can be in the form of data backup or system backup. Backup can be placed on site of Data Center location and/or off site of alternative locations.

13. *Backup Site*:

Storage location of backup computer and files separate from Data Center*.*

12*. Backlog project*:

The presence of delayed application system development project.

13*. Business Continuity Management* (BCM):

A joint and entire management process to ensure that Bank's operations remain functional even in the event of disturbance/disaster, to protect the interest of stakeholder*.*

14*. Business Continuity Plan* (BCP):

A written document which contain an arrangement of planned and coordinated activities regarding steps to decrease risks, responses on the impacts of disturbances/disasters, and recovery process so for Bank's operations and services to customers still operating. The said written action plan involves every Information Technology (IT) resource including human resources which support business functions and operational activities critical to the Bank.

15. *Business Impact Analysis* (*BIA*):

A process to recognize the impacts from the unavailability of support from all resource. In this phase includes identification of various occurrences which can cause certain impact on the continuity of operational and financial activities, on human resources and on the reputation of the company. BIA is a form of critical steps in the development of BCP.

***16. Business Recovery Center/Crisis Center/Business Resumption Center*:**
A location used as the centre of business activities in the time of recovery after the occurrence of disaster.

17. *Client Server*:
A computer architecture where there are 2 types of entry point in the form of a client and a server. Every client can send a data request to one server or more connected to each other. The server then accepts, processes and responds to said data request.

18*. Cold Sites*:
An alternative location (DRC) which only have basic facilities (such as: electricity, AC and rooms) and has not possess a compatible computer configuration as well as a complete backed up data as it were in DRC hot sites. This location is ready to receive a replacement of necessary computer equipments if a user must move from the Data Center to an alternative location. For that, if this location is to be used, it will require additional time before being ready to be used to replace Data Center in the event of Disaster.

17*. Communicative E-Banking*:
A service of a Bank to customers through an electronic media in the form of communication or by interacting with the Bank in limited means and without a transaction execution.

18. *Contingency Plan*:
A procedure containing plans of manual steps required to be done by business units to run business operations in the time of recovery.

19*. Controller (Host-Front End)*:
telecommunication control unit is a type of mini computer which function is to control the performance of existing hardware and software in a system such as computer terminal / ATM, communication network or other computer facilities.

20*. Cost and Benefit Analysis*:
An analysis of comparison between investment cost and obtained profits from every alternative selection of service provider. The result of this analysis becomes one of the Bank's considerations to decide in outsourcing or selection of service provider.

21*. Cybersquating*:
Registration or the use of website address or name of a domain with bad intentions, which are to abuse or gain profits from the use of trademarks by unauthorized parties.

22. *Database*:
A base for data which is a representation of facts related to each other, stored together in a certain way and with no unnecessary redundancy, to meet various requirements. Data need to be stored in a database for further information providing. Data in a database need to be organized in a certain way, so for the information as a result are of good quality. A good database organization is also useful for its storage capacity efficiency. In the same meaning, can also be understood as a cluster of information arranged in a certain way to be accessible by a particular software. A database consists of sections called field and record which are stored in a file. A field is the smallest unit of information in a database. A cluster of field related to each other will form a record.

23*. Data Center*:
The main facility for Bank's data processing which consist of hardware and software to support Bank's operations in continuity.

24*. Defacing*:
A hacker's attempt to attack and change the display or the content of a website.

25. DES (*Data Encryption Standard*):
An encryption standard based on block cipher algorithm. This standard has long been used and often considered unable to provide adequate security.

26*. Denial of Service Attack*:
Attacks on information technology system causing it to become slow or non-functional at all, such as by making as though the bandwidth or computer disk space are fully used, through disturbances on server as well as disturbances on service providing to another system or user.

27*. Digital Certificate*:
Electronic identity used to identify and verify that a message was sent by an authorized person or company, and only read by an also authorized party. Digital certificate is published by a third party called "certification authority" (CA) such as Verisign (www.verisign.com) and Thawte (www.thawte.com).

28. *Digital signatures*:
Information of certain signs in digital form which can ensure the authentication of sender, data integrity, and is undeniable.

29*. Disaster Recovery Plan (DRP)*:
Documents that consist of plans and steps to regain/recover data access, hardware and software necessary for Bank to be able to run critical business operations after a disaster. DRP stresses on the aspect of technology.

30*. Disaster Recovery Center* (*DRC*):
An alternate location useable when Data Centers suffers disturbances or is non-functional as a result of a disaster, amongst others are the absence of electricity to the computer room, fire, explosion or damage on computers, which is used temporarily during the recovery of Bank's Data Center to safeguard business continuity.

31. *Disposal Media Backup*:
Destruction process of a backup media which has passed its retention period and no longer used.

32. *Down Time*:
The duration of a system being non-functional and unusable because of disturbances on hardware, software and communication.

33*. Due Diligence*:
A process to obtain complete information about service providers to assess the reputation, operational capability, managerial, financial condition, future development strategy and capability in following technology advances.

34*. E-money* or *stored value* or *prepaid card*:
Products used in the mechanism of payment system through point of sales (merchant), transfer between two electronic media or computer network using money value stored in a card or in said products.

35*. Electronic Data Capture/Point of Sales Terminal*:
A hardware or computer terminal in the form of cash register or debit/credit verification terminal that reads the information on the card's magnetic stripe. Cards regarding transaction data at the place of trade (merchant), transmit data to acquirer for verification and processing.

36*. Electronic Fund Transfer*:
Funds transfer between accounts through a payment system using electronic media. EFT is usable for financial transaction through telephone, computer terminal, etc.

37. Encryption:

Tools to achieve data security by translating the data using a key (password). Encryption prevents the password or the key so as to be unreadable in the configuration file.

38*. Escrow Agreement*:

An agreement that enables delivery of rights to software buyers so as to be able to obtain the most recent version source code when the company who made the application system is inoperative, for example because of being declared bankrupt.

39*. Exception Handling*:

A mechanism to handle uncalled-for conditions which can change the normal course of an application system.

40*. Firewall*:

Tools to safeguard network security which conducts monitoring and selection on data/information traffic through the network as well as separating private network from public network. These tools can be used to protect computers that are connected to a network from attacks which can compromise internal computers which will further cause data corruption and/or denial of service for authorized users.

41*.Full System Back up*:

system backup which includes the entire system being used.

42. *Gateway*:

Points in a network which function as an entrance to other networks or to connect one network to another. Gateway can be in the form of a computer which regulates and controls network traffic.

43. *Hardcopy*:

Copies of computer data/information in a written form or what is known as a printout.

44. *Hardening*:

Is a process/method to secure a system from various threats of disturbances. The methods used include, amongst others, deactivating unnecessary services as well as unnecessary username or login, developing intrusion detection system, intrusion prevention system, and firewall.

45. *Hash Function*:

A way to change data (usually in the form of messages or files) to become a certain number which can be used by computers to reproduce the original data.

46*. Hot Card File*:
Files that store information about magnetic cards that must be held by machines such as ATM, because said cards do not fulfill the requirements to be operative.

47*. Hot Sites*:
Alternative locations (DRC) with complete computer configuration (hardware, network, system software and applications) and compatible with the Data Center. In general it can be functional immediately after the occurrence of disaster, so data is continuously being backed up using live connection between Data center and DRC.

48. *Hub*:
A Tool which connect several cables to a network and continuing data / information to all address of network point or tools aimed at.

49*. Informational E-Banking*:
Bank's service to customers through electronic media such as internet, mobile phone, telephone, etc, and absent of transaction execution.

50*. Interoperability*:

a. ability of software or hardware on various types of machine from many vendors to communicate to each other.
b. ability to exchange and use information (usually in one large network which consist of several various local networks).

51*. Interface / Integration Testing*:
Testing by quality assurance and end user to test the interface of integrated software components, including their relation with other systems.

52*. IT Control*:
Control of Information Technology which include general control and integrated application control to support business process. IT general control is necessary to enable the implementation of application control function. Bank general control include control in Bank's IT management and organization, access control of logical or physical means, conduct of DRP/BCP, etc. Application control is necessary to ensure the comprehensiveness and accuracy in every stage of information processing. Application control is integrated with the application system used for transaction processing.

53*. Key logger*:
A threat in the form of software or hardware used to obtain information (PIN, password) typed on keyboards (usually in an internet café).

54*. Library*:
A cluster of software or data which have a certain function and are stored as well as ready to use.

55*. Logic Bomb*:
A code that is intentionally inserted in a software system which at a certain condition will conduct a number of damaging functions.

56*. Man-in-the-middle-attack*:
A type of attack on information technology systems where a hacker/attacker intercepts a message and/or then changes the content of the message and sends it to the recipient. Hacker/attacker will use a program that looks as a server to the client, and as a client to the server.

57*. Maximum Tolerable Outage / Recovery Time Objective*:
Tolerable time duration when a system is not functional because of a disturbance. RTO indicates the earliest point in time necessary for business operational to operate again after the occurrence of a disaster.

58*. Mobile Banking*:
A service that enables Bank's customers to have banking transactions through hand phones. Mobile banking generally used through a sms or mobile internet, but can also use a special program downloaded through a hand phone.

59*. Modem (Modulator Demodulator)*:
A device placed between communication machine and telephone line to enable digital pulse transmission. A telephone line can only transmit analog signal and not digital signal like the one from computers. Modulator will change bit pulse to notes and send it through communication network, on the other hand a demodulator will change it to suitable bit.

60*. Network interface*:
Point of interconnection between user terminal, machines, or a network to another network.

61*. Non-repudiation*:
A way to ensure the authenticity of sender and recipient so there can not be any parties able to deny.

62*. Off-line*:
A system or computer with no network connection or unable to communicate with other systems or computers.

63*. Off the shelf*:
Provided as it is, created without any special order.

64*. Orphan Account*:
Account of a user that has gone out from an organization.

65*. Outsourcing*:
The use of other parties (external) in the carrying-out of Bank’s information technology which causes the Bank to have a dependency to the service provided by said other parties in continuity or in a certain period.

66*. Parallel Distributed Computing*:
A distributed system which consists of a group of computers connected in a network, with joint software so every computer can share resources of hardware, software and data. This system can coalesce geographical differences, increases performance and interaction as well as suppresses cost.

67*. Password*:
Codes or special symbols to secure computer systems for identifying individuals accessing data, program or computer application being used.

68*. Patch*:
A cluster of codes added to software to repair an error, usually is in the form of temporary correction between two versions of software.

69*. Patch Management*:
System management which includes the process of obtaining, testing and installations of various patch used to repair a program.

70. Physical Security:
A security system to prevent access by unauthorized parties on an area of computerization as well as on supporting equipments/facilities.

71. Logical Security:
A security system to prevent access by unauthorized parties on a computer system and the information inside which include the use of user ID, password, etc.

72*. Personal Identification Number* (PIN):
A series of unique digits consist of letters, numbers or ASCII codes which is used to identify c computer users, ATM users, internet banking, mobile banking, etc.

73. *Switching Company*:
A company which provide electronic banking services to Banks and financial institutions, amongst others in the management of computer hardware, telecommunication network, information as well as transactions records of the customers of said Banks and financial institutions.

74*. Phising*:
One of the technical forms of social engineering to obtain someone's confidential information illegally. Phising can be in the form of fake e-mail as though from a Bank, credit card company, etc. to obtain information such as PIN, password, etc.

75*. Phone Banking*:
A service which enables Bank's customers to conduct banking transactions through a telephone.

76*. Piggybacking*:
(i) An action where a person enters a room by following another person with the authorization to access said room;
(ii) A way to intrude or to change a transmission by attaching to an authorized telecommunication network.

77. Magnetic Tape:
A recording tape used as a data storage media. Every character is written across the tape's width in the form of dots containing magnetism. Reading from and typing to the tape are done by moving the surface of the tape across a read/write head of a tape drive.

78*. Platform*:
Hardware of software such as computer architecture, operation system or programming language which enables an application to be operative.

79*. Point of Sales*:
Hardware or a computer terminal in the form of cash register or debit/credit verification terminal which can receive information on retail sales at the place of the sale and inserting data as input to a computer.

80. *Power User*:
User id with extensive authorization.

81*. Process Control*:
Control by service providers mainly related to the process of services given to Banks to ensure the quality of service from the view of confidentiality, integrity and availability*.*

82*. Public Key Infrastructure*:
A management/regulation where a trusted third party provides a detailed assessment and ensures the validity of an identity.

83. *Rapid Application Development* (RAD):
A methodology of system development which consist of repeating development and prototyping development that are quickened so to cause the benefit, feature and program execution speed not to be optimal.

84. *Request for Proposal (RFP)*:
A process of request proposal to service providers in accordance to Bank's requirements for the purpose of selection. Submitted proposal must be able to answer in detail the Bank's requirements which have been defined as mentioned in the document of business requirement or target operating model.

85*. Restore*:
Return to the initial function or condition before the occurrence of disaster.

86. *Restricted area*:
An area which is only accessible by authorized persons.

87*. Router*:
Network equipment which continue a package of data/information and choose the best route to convey said data/information.

88*. Service Level Agreement*:
A part of an agreement contract where the expected service level providing are determined, and usually also includes agreed performance standard (service level) or time service providing target.

89. *Social Engineering*:
A deceitful technique through social behavior done by hackers to deceive people to give confidential information such as PIN, password, etc.

90*. Softcopy*:
Copies of data or documents in the form of electronic files.

91*. Software Patch*:
A program made by vendor to increase performance and security of its software product, of software in the form of operation system, database, application development tools, etc.

92*. Source Code*:
Software program instructions written in a certain form (language) and readable by human.

93*. Spoofing*:
A condition where a person or program can assimilate another person or program by falsifying data for the purpose of gaining certain benefits.

94. *Spy ware*:
Software which collect sensitive information about users without the acknowledgement or permission from the users.

95. *Stress Testing*:
A type of testing in a development which use various scenarios, such as a bad condition. Stress testing is necessary in relation to performance, load balancing, especially for complex application.

96*. Subcontractor*:
Other service providers assigned by one service provider already in a contract with a Bank.

97. *Switch*:
A tool in a network which continues information packages to an address or tools aimed for.

98. *System*:
A work network from connected procedures, gathering to conduct an activity or to accomplish a certain target.

99. *System Development Life Cycle*:
A cycle of system development which includes the following steps: (1) system planning, (2) system analysis, (3) system design, (4) system selection, (5) system implementation, (6) system maintenance.

100. *System Source*:
One of the points of information necessary in storage media inventory, which is the indication of which system the data is obtained from.

101*. System Testing*:
Testing done by quality assurance to test the functionality of the entire application system, including every object in said application system.

102*. System Log*:
A file in a computer which stores information about the activities of a system or a computer.

103. *Technical Reference*:
Technical guideline of a database application which contain, amongst others, explanation about database structure which consist of tables and fields including the relation between tables, in the form of entire relationship diagram (ERD).

104*. Transactional E-Banking*:
Bank's service to customers through electronic media where there are transaction executions.

105*. Trojan Horse*:
A program of damaging nature slipped in by hackers in a program known to users. Its replication or distribution is activated by said known program through the "social engineering" method.

106*. Unit Testing*:
Testing by developers to test the functionality of small modules in a software program.

107. *Upload* and *Download*:
Electronic data transfer between two computers or similar systems.

108. *User Acceptance Test*:
Final testing by users to test the functionality entirely and the interoperability of an application system.

109*. User Log*:
A file in a computer which stores information about user activities such as the time of login and logout.

110. Virus:
A program of damaging nature which will be active with the assistance of people (executed), replicating itself, its spread is by people, such as from the act of copying, usually through e-mail attachment, games, pirated programs, etc.

111*. War Driving*:
An action to obtain wi-fi network (wireless local area network) by using equipments which is able to detect the signal of wi-fi network, such as a laptop or PDA.

.

112*. Warm Sites*:
Alternative locations (DRC) which have a section of configuration from the Data Center and generally only consist of network connection and several supporting equipments without a main computer. The system will not move automatically but there is still a manual process even if it is done at a minimum.

113. *Web Site*:
A web page or information conveyed through a web browser or a cluster of web page planned, presented and connected to each other to form an information source and/or to conduct the function of transaction.

114*. Worm*:
A computer program designed to automatically self-replicate by attaching to e-mails or becoming a part of network messages. Worm attacks networks and affect the denseness of bandwidth being used so as to obstruct the rate of data transmission in a network.